Congratulations! You passed!

Grade received 95%

Weekly challenge 3

Latest Submission Grade 95%

To pass 80% or higher

Go to next item

Quiz • 50 min

Review Learning Objectives

1. What do network-level Denial of Service (DoS) attacks target? **1 / 1 point**

- Network bandwidth
- Commonly used software applications
- The personal information of employees
- All hardware within an organization

Correct

Submit your assignment

Try again

Due 3 Jun 23, 11:59 PM +08 Attempts 3 every 24 hours

Receive grade

Your grade 95%

View Feedback

We keep your highest score

To Pass 80% or higher

Like Dislike Report an issue

2. Which of the following statements accurately describe Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks? Select three answers. **0.75 / 1 point**

- [x] In both DoS and DDoS attacks, every part of the network must be overloaded for the attacks to be successful.

  This should not be selected
  Please review the video about DoS attacks.

- [x] A network device experiencing a DoS attack is unable to respond to legitimate users.

  Correct

- [x] A DDoS attack involves multiple hosts carrying out the attack.

  Correct

- [x] A DoS attack involves one host conducting the attack.

  Correct

3. A security manager is training their team to identify when a server has experienced a SYN-flood attack. What might indicate to the team members that their organization is at risk? **1 / 1 point**

- (•) The server has stopped responding after receiving an unusually high number of incoming SYN packets.
- ( ) The port numbers in the data packets are incorrect.
- ( ) An oversized ICMP packet is sent to the network server.
- ( ) A large number of ICMP packets are delivered to the organization's servers.

Correct

4. Fill in the blank: The DoS attack _____ occurs when a malicious actor sends an oversized ICMP packet to a server. **1 / 1 point**

- ( ) smurf
- ( ) SYN flood
- (•) Ping of Death
- ( ) on-path

Correct

5. Which of the following statements correctly describe passive and active packet sniffing? Select three answers. **0.75 / 1 point**

- [x] Passive packet sniffing allows malicious actors to view the information going in and out of the targeted device.

  Correct

- [x] A company can avoid using unprotected Wi-Fi to help protect itself from packet sniffing.

  Correct

- [x] Passive packet sniffing enables attackers to change the information a packet contains.

  This should not be selected
  Please review the video about malicious packet sniffing.

- [x] Active packet sniffing may enable attackers to redirect the packets to unintended ports.

  Correct

6. As a security professional, you implement safeguards against attackers changing the source IP of a data packet in order to communicate over your company's network. What type of network attack are you trying to avoid? **1 / 1 point**

- (•) IP spoofing
- ( ) Passive packet sniffing
- ( ) Ping of Death
- ( ) Active packet sniffing

Correct

7. Fill in the blank: To reduce the chances of an IP spoofing attack, a security analyst can configure a _____ to reject all incoming traffic with the same source IP addresses as those owned by the organization. **1 / 1 point**

- ( ) HTTPS domain address
- (•) firewall
- ( ) demilitarized zone
- ( ) VPN

Correct

8. In which attack would malicious actors gain access to a network, put themselves between a web browser and a web server, then sniff the packet to learn the devices' IP and MAC addresses? **1 / 1 point**

- ( ) Malware attack
- ( ) Smurf attack
- ( ) Packet flooding attack
- (•) On-path attack

Correct

9. Fill in the blank: The _____ network attack occurs when an attacker intercepts a data packet in transit, then repeats it at another time. **1 / 1 point**

- ( ) on-path
- ( ) smurf
- ( ) SYN flood
- (•) replay

Correct

10. Which attack involves an attacker sniffing an authorized user's IP address and flooding it with packets? **1 / 1 point**

- ( ) Replay attack
- (•) Smurf attack
- ( ) On-path attack
- ( ) Ping of Death

Correct