Congratulations! You passed!

Grade received 95%

Weekly challenge 3

Latest Submission Grade 95%

To pass 80% or higher

Quiz • 50 min

Retake the assignment in **23h 56m**

Go to next item

Review Learning Objectives

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

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

Correct

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**

- [ ] In both DoS and DDoS attacks, if any part of the network is overloaded, the attacks are successful.
- [x] A DDoS attack may use multiple devices in different locations to flood the target network with unwanted traffic.

Correct

- [ ] A DoS attack involves multiple hosts carrying out the attack.
- [x] A DoS attack targets a network or server.

Correct

You didn't select all the correct answers

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**

- A large number of ICMP packets are delivered to the organization's servers.
- 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.

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**

- on-path
- Ping of Death
- smurf
- SYN flood

Correct

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

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

Correct

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

Correct

- [ ] Passive packet sniffing enables attackers to change the information a packet contains.
- [x] Active packet sniffing may enable attackers to redirect the packets to unintended ports.

Correct

6. As a security professional, you research on-path, replay, and smurf attacks in order to implement procedures that will protect your company from these incidents. What type of attack are you learning about? **0 / 1 point**

- Ping of death
- SYN flooding
- IP spoofing
- Packet sniffing

Incorrect
Please review the video about impersonation.

7. What are some common IP spoofing attacks? Select all that apply. **1 / 1 point**

- [x] on-path attacks

Correct

- [x] replay attacks

Correct

- [x] smurf attacks

Correct

- [ ] KRACK attacks

8. In which attack would a malicious actor place themselves in the middle of an authorized connection and intercept the data in transit? **1 / 1 point**

- Malware attack
- Packet flooding attack
- Smurf attack
- On-path attack

Correct

9. Fill in the blank: The _____ network attack occurs when a malicious actor takes a network transmission that was sent by an authorized user and repeats it at a later time to impersonate that user. **1 / 1 point**

- smurf
- replay
- on-path
- SYN flood

Correct

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

- Smurf attack
- Ping of Death
- Replay attack
- On-path attack

Correct