

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

1 / 1 point

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

☒ Correct

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

0.5 / 1 point


- ☐ A DDoS attack involves multiple hosts carrying out the attack.
- ☒ A network device experiencing a DoS attack is unable to respond to legitimate users.

☒ Correct

- ☒ A DoS attack involves one host conducting the attack.

☒ Correct

- ☒ 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](#) .

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.
- ☐ A large number of ICMP packets are delivered to the organization’s servers.
- ☐ The port numbers in the data packets are incorrect.
- ☐ An oversized ICMP packet is sent to the network server.

☒ Correct

4. Which type of attack occurs when a malicious actor sends an oversized ICMP packet to a server?

1 / 1 point

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

☒ Correct

5. Which type of packet sniffing allows malicious actors to view and read data packets in transit?

1 / 1 point

- ☒ Passive packet sniffing
- ☐ Active packet sniffing
- ☐ IP packet interception
- ☐ Hardware packet sniffing

☒ 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?

1 / 1 point

- ☐ SYN flooding
- ☒ IP spoofing
- ☐ Ping of death
- ☐ 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
- ☐ VPN
- ☒ firewall
- ☐ demilitarized zone

✓ **Correct**

8. A malicious actor impersonates a web browser or web server by placing themselves between two devices, then sniffing the packet information to discover the IP and MAC addresses. Which type of attack is this?

1 / 1 point

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

- ☐ SYN flood
- ☐ smurf
- ☒ replay
- ☐ on-path

✓ **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
- ☐ Ping of Death
- ☐ On-path attack

✓ **Correct**