- **Introduction to network intrusion tactics**
- **Secure networks against Denial of Service (DoS) attacks**
- **Network attack tactics and defense**
- **Review: Secure against network intrusion**
- **Video:** Wrap-up
  44 sec
- **Reading:** Glossary terms from week 3
  10 min
- **Quiz:** Weekly challenge 3
  10 questions

Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Go to next item

Weekly challenge 3

Quiz • 50 min

Review Learning Objectives

Submit your assignment

Due Jun 25, 11:59 PM +08 **Attempts** 3 every 24 hours

Try again

Receive grade

To Pass 80% or higher

Your grade
100%

View Feedback
We keep your highest score

Like **Dislike** **Report an issue**

1. What is the main objective of a Denial of Service (DoS) attack? **1 / 1 point**

○ Repeatedly send ICMP packets to a network server

● Disrupt normal business operations

○ Simulate a TCP connection and flood a server with SYN packets

○ Send oversized ICMP packets

✓ **Correct**

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

☑ A network device experiencing a DoS attack is unable to respond to legitimate users.

✓ **Correct**

□ In both DoS and DDoS attacks, every part of the network must be overloaded for the attacks to be successful.

☑ A DDoS attack involves multiple hosts carrying out the attack.

✓ **Correct**

☑ A DoS attack involves one host conducting the attack.

✓ **Correct**

3. A security team discovers that an attacker has taken advantage of the handshake process that is used to establish a TCP connection between a device and their server. Which DoS attack does this scenario describe? **1 / 1 point**

● SYN flood attack

○ ICMP flood

○ Ping of Death

○ On-path attack

✓ **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**

○ SYN flood

● Ping of Death

○ smurf

○ on-path

✓ **Correct**

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

☑ Active packet sniffing may enable attackers to redirect the packets to unintended ports.

✓ **Correct**

□ Passive packet sniffing enables attackers to change the information a packet contains.

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

✓ **Correct**

☑ Passive packet sniffing allows malicious actors to view the information going in and out of the targeted device.

✓ **Correct**

6. As a security professional, you take steps to stop an attacker from changing the source IP of a data packet in order to impersonate your authorized system. What type of network attack are you working to prevent? **1 / 1 point**

● IP spoofing

○ Ping of Death

○ Passive packet sniffing

○ 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**

○ VPN

● firewall

○ demilitarized zone

○ HTTPS domain address

✓ **Correct**

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

● On-path attack

○ Smurf attack

○ Packet flooding attack

✓ **Correct**

9. Fill in the blank: The _____ network attack occurs when an attacker delays a data packet after intercepting it in transit. **1 / 1 point**

● replay

○ on-path

○ SYN flood

○ smurf

✓ **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**