Knowledge Check Quiz Related Topic Week 3 (Distributed Denial of Service)

Due Feb 6 at 11:59pm **Points** 8 **Questions** 8
Available until Feb 6 at 11:59pm **Time Limit** None

Instructions

Answer the following questions on the related topic material this week.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	11 minutes	8 out of 8

Score for this quiz: **8** out of 8
Submitted Jan 19 at 1:37pm
This attempt took 11 minutes.

Question 1

1 / 1 pts

What does the acronym **DDoS** stand for?

○ Dramatic Decision of Significance

○ Dedicated Data on Server

○ Digital Database of Systems

Correct! ● Distributed Denial of Service

Question 2

1 / 1 pts

What is the definition of a **HTTP GET Flood** as a DDoS technique to cause the victim's system to consume bandwidth and become unavailable to legitimate users?

○ Send connection requests with false packets that do not acknowledge open connection

○ Send excessive number of pings or packets

○ Send packets to random ports consuming victim with responses to unreachable destinations

Correct!

● Send continuous requests for website server connections

Question 3

1 / 1 pts

What is the definition of an **Internet Control Message Protocol (ICMP) Flood** as a DDoS technique to cause the victim's system to consume bandwidth and become unavailable to legitimate users?

○ Send continuous requests for website server connections

Correct!

● Send excessive number of pings or packets

○ Send connection requests with false packets that do not acknowledge open connection

○ Send packets to random ports consuming victim with responses to unreachable destinations

Question 4

1 / 1 pts

What is the definition of a **TCP Synchronize (SYN) Flood** as a DDoS technique to cause the victim's system to consume bandwidth and become unavailable to legitimate users?

○ Send continuous requests for website server connections

○ Send packets to random ports consuming victim with responses to unreachable destinations

Correct!

● Send connection requests with false packets that do not acknowledge open connection

○ Send excessive number of pings or packets

Question 5

1 / 1 pts

What is the definition of a **User Datagram Protocol (UDP) Flood** as a DDoS technique to cause the victim's system to consume bandwidth and become unavailable to legitimate users?

○ Send excessive number of pings or packets

○ Send continuous requests for website server connections

○ Send connection requests with false packets that do not acknowledge open connection

Correct!

● Send packets to random ports consuming victim with responses to unreachable destinations

Question 6

1 / 1 pts

Which of the following is one of the **recommendations and mitigation strategies** offered in the Guide to DDoS Attacks?

Correct!

● Configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies

○ Block traffic from unknown IP addresses

○ Minimize port and packet sizes to prevent a single IP address from too much access

○ Apply all patches as soon as the vendor makes them available

Question 7

1 / 1 pts

Which type of DDoS attack occurs when **attackers spoof their IP address to pose as the intended victim** and then send legitimate requests to legitimate public-facing servers?

○ Standard

○ Botnets

○ Amplification

Correct!

● Reflection

Question 8

1 / 1 pts

What is the difference between a SYN flood and a UDP flood?

○ UDP flood requires holding communication open while waiting for confirmation

○ SYN flood requires response to sender of packet with ICMP Destination Unreachable packet

Correct!

● UDP flood is faster than a SYN flood because large number of packets are requesting various destination ports

○ UDP flood is the simplest and most common form of a DDoS attack

Quiz Score: **8** out of 8