Exercise Week 3: Distributed Denial of Service Attack

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

Instructions

This exercise asks questions about a hypothetical Distributed Denial of Service attack.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	11 minutes	5 out of 6

Score for this quiz: **5** out of 6
Submitted Jan 19 at 1:50pm
This attempt took 11 minutes.

Question 1

1 / 1 pts

A DDoS attack is launched using IoT devices infected with malware. The malware allows the attacker to remotely control these IoT devices.

Which term can we use to describe this collection of IoT devices?

- Content Management System
- Loopback
- Transmission Control Protocol
- Botnet

Correct!

Question 2

1 / 1 pts

The attacker commands all of these IoT devices to request a connection with the victim's server. When the server acknowledges the connection request, the malware infected IoT devices do not respond. This causes the victim's server to wait until the request times out. Because so many requests are being made and not completed, the server becomes overwhelmed and is not available to legitimate users.

What kind of DDoS attack is this?

- NTP Reflection
- SQL Injection
- SYN Flood

Correct!

- Pingback Amplification

Question 3

0 / 1 pts

What could the victim do before the DDoS attack to prevent the attack or minimize its impact?

- Enable firewall logging of accepted and denied traffic

ou Answered

- Create a plugin for the website that manually disables pingback functions

Investigate network logs to identify the source of the attack

orrect Answer

Enable SYN cookies to force the firewall to validate connections

Question 4

1 / 1 pts

Next, the attackers command the compromised IoT devices to falsify their IP address to pose as the victim's address. The compromised IoT devices then send connection requests to real servers and websites, overwhelming the victim's server with all of the responses.

What type of DDoS attack is this?

Correct!

Reflection

Amplification

Pingback

Push

Question 5

1 / 1 pts

Next, the attackers send requests for a large amount of data from a real server to be sent to the victim's server.

What type of DDoS attack is this?

- Pingback
- Reflection

Correct!

- (selected) Amplification
- Push

Question 6

1 / 1 pts

What can the victim do during the attack to respond?

- Establish and regularly validate baseline traffic patterns
- Apply all vendor patches after appropriate testing
- Configure firewall to use ingress and egress filters

Correct!

- (selected) Filter out packets likely to be part of the attack

Quiz Score: **5** out of 6