**Expeiment** Ingress Network Attack - Simulating a DDoS Attack on Exposed Services

**Load Testing (External)**

A **Distributed Denial-of-Service (DDoS) attack** is a cyberattack where an attacker overwhelms a website, server, or network resource with **malicious traffic**, causing it to crash or become unresponsive. This prevents legitimate users from accessing the service.

**Types of DDoS Attacks:**

1. **TCP SYN Flood** – Exploits the TCP handshake process, leading to incomplete connections.
2. **UDP Flood** – Overwhelms the target with a large number of UDP packets.
3. **HTTP Flood** – Sends excessive HTTP requests to exhaust server resources.

**Ways to Simulate a DDoS Attack in Chaos Mesh**

1. **Network Bandwidth Throttling** – Restricts available bandwidth to mimic high network congestion.
2. **Packet Loss Simulation** – Drops packets randomly to simulate network instability.
3. **Network Delay (Latency Injection)** – Introduces artificial latency to slow down responses.
4. **Network Partitioning** – Simulates network segmentation, blocking communication between services.

**Other Tools for Simulating DDoS Attacks**

* **Locust** – A load-testing framework that allows custom attack scenarios.

**Implementation Details**

I applied a **parallel YAML configuration**, which impacted **network latency** while simulating user load:

**Test Scenarios:**

1. **Scenario 1:**
   * **Concurrent Users:** 50
   * **Requests per Second:** 0.5 (1 user per 2 seconds)
   * **Duration:** 2 minutes
2. **Scenario 2:**
   * **Concurrent Users:** 100
   * **Requests per Second:** 0.25 (1 user per 4 seconds)
   * **Duration:** 4 minutes

* **Expected outcome:**
* allowed the some user requests
* Running the **DDoS YAML configuration** resulted in increased **latency**, allowing only some requests to go through.