**Experiment:** Network Egress Leak

**Type:** Network Chaos   
**Description:** Test whether pods can bypass network policies to access external systems**.**

**Introduction**

The goal of this experiment is to evaluate if pods can bypass network policies to access external systems and simulate load testing using Locust. This will help identify potential security loopholes in egress policies and assess system resilience.

**Implementation**

We will use Chaos Mesh to disrupt network policies and observe their impact on egress traffic. After the disruption, we will verify if the pod can regain access to external systems, indicating a potential egress policy bypass**.**

**Steps to Follow:**

1. Apply a Network Policy – Restrict egress traffic for a specific pod.
2. Verify Policy Enforcement – Ensure the network policy is correctly configured and active.
3. Check Egress Connectivity (Blocked) – Confirm that outbound traffic is restricted as expected.
4. Disrupt the Network Policy Using Chaos Mesh – Temporarily disable the policy to observe the effects.
5. Check Egress Connectivity (Success) – Verify if the pod regains access to external systems, indicating a possible security gap.
6. Install Locust for Load Testing – Use Locust, a modern load-testing framework, to stress test API performance under different network conditions.

cd /root/hymavathi/networkegress

   ./script.sh

**Expected Outcome**

* The outbound traffic should be blocked initially due to the applied network policy.
* I getting a network disruption error