313-Recitation 10: Gremlin

Goal: During this recitation, students will learn how to use Gremlin to run a chaos engineering-style attack against a microservice application.

Task:

0. Make sure you have *no* Docker containers running for PostgreSQL or Mayan-EDMS before you start this exercise. Confirm this with `docker ps` and remove any currently running instances of Mayan-EDMS and PostgreSQL.
1. Create an account with Gremlin (http://gremlin.com). When asked for the organization and team, enter Carnegie Mellon University for both – it will tell you that permission will be granted by the team owner – I will grant permission.
2. Start a new instance of the Gremlin-enabled Mayan-EMDS.
```
docker run -d \
-p 8000:8000 \
--cap-add=NET_ADMIN \
--cap-add=SYS_BOOT \
--cap-add=SYS_TIME \
--cap-add=KILL \
-e GREMLIN_ORG_ID="80fc5b45-ab32-5544-9f54-071e5d6436af" \
-e GREMLIN_ORG_SECRET="b92a9ffb-aa2e-4ee4-aa9f-fbaa2efee449" \
-it cmeiklejohn/mayanedms:3.2.7
```
3. Go to the “Clients” tab in Gremlin and find the identifier for your client. You should be able to correlate the container name (see using `docker ps`) and the `local-hostname` of the container that's running. For all of the following attacks, target only your container and not your classmates, please.
4. Run your first attack using the Attack tab in the menu:
    a. Select a State Attack and choose the Attack type of "Shutdown."
    b. What happens to Mayan-EDMS?

    c. What happens to your container?

5. Let's try another attack, but instead, let's simulate an outage using an attack.
    a. Select Scenario.
    b. Type a name and description of the outage.
    c. Add an attack: Resource, CPU.
    d. Scroll back up and create a hypothesis of what you think will happen to Mayan.
    e. What is your hypothesis?

    f. Run your attack scenario!

g. What happened to Mayan-EDMS?

h. What happened to your container?

i. Was your hypothesis correct?

6. Terminate your Docker instances. Let's try an example using Mayan-EDMS with PostgreSQL.
   a. You may have to adjust the docker-volumes path as you did in recitation 2.
   b. First, run PostgreSQL:

```
docker run -d \
-p 5432:5432 \
-e POSTGRES_USER=mayan \
-e POSTGRES_DB=mayan \
-e POSTGRES_PASSWORD=mayanuserpass \
-v /docker-volumes/mayan-edms/postgres:/var/lib/postgresql/data \
--cap-add=NET_ADMIN \
--cap-add=SYS_BOOT \
--cap-add=SYS_TIME \
--cap-add=KILL \
-e GREMLIN_ORG_ID="80fc5b45-ab32-5544-9f54-071e5d6436af" \
-e GREMLIN_ORG_SECRET="b92a9ffb-aa2e-4ee4-aa9f-fbaa2efee449" \
-it cmeiklejohn/mayanedms-postgresql:9.6
```

   c. Now, run Mayan-EDMS:

```
docker run \
-p 8000:8000 \
-e MAYAN_DATABASE_ENGINE=django.db.backends.postgresql \
-e MAYAN_DATABASE_HOST=172.17.0.1 \
-e MAYAN_DATABASE_NAME=mayan \
-e MAYAN_DATABASE_PASSWORD=mayanuserpass \
-e MAYAN_DATABASE_USER=mayan \
-e MAYAN_DATABASE_CONN_MAX_AGE=0 \
-v /docker-volumes/mayan-edms/media:/var/lib/mayan \
--cap-add=NET_ADMIN \
--cap-add=SYS_BOOT \
--cap-add=SYS_TIME \
--cap-add=KILL \
-e GREMLIN_ORG_ID="80fc5b45-ab32-5544-9f54-071e5d6436af" \
-e GREMLIN_ORG_SECRET="b92a9ffb-aa2e-4ee4-aa9f-fbaa2efee449" \
-it cmeiklejohn/mayanedms:3.2.7
```

   d. Create a scenario that targets *only* PostgreSQL using the shutdown attack.
   e. What was your hypothesis?

f. What happened to Mayan-EDMS?

g. What happened to PostgreSQL?

h. What happened to your container?

i. Was your hypothesis correct?

7. **Rerun the previous experiment, but instead, use the following command to start PostgreSQL:**
   a.
```
docker run -d \
   --restart=always \
   -p 5432:5432 \
   -e POSTGRES_USER=mayan \
   -e POSTGRES_DB=mayan \
   -e POSTGRES_PASSWORD=mayanuserpass \
   -v /docker-volumes/mayan-edms/postgres:/var/lib/postgresql/data \
   --cap-add=NET_ADMIN \
   --cap-add=SYS_BOOT \
   --cap-add=SYS_TIME \
   --cap-add=KILL \
   -e GREMLIN_ORG_ID="80fc5b45-ab32-5544-9f54-071e5d6436af" \
   -e GREMLIN_ORG_SECRET="b92a9ffb-aa2e-4ee4-aa9f-fbaa2efee449" \
   -it cmeiklejohn/mayanedms-postgresql:9.6
```
   b. Create a scenario that targets *only* PostgreSQL using the shutdown attack.
   c. What was your hypothesis?

   d. What happened to Mayan-EDMS?

   e. What happened to PostgreSQL?

   f. What happened to your container?

   g. Was your hypothesis correct?