## ****Instructions to Run Model Stealing Attack****

### ****Step 1: Activate the Environment****

Run the following command to activate the virtual environment:

# Replace 'your\_env' with the actual environment name

source your\_env/bin/activate # For Linux/macOS

your\_env\Scripts\activate # For Windows (Command Prompt)

### ****Step 2: Deploy the Model on the Server****

Execute the deployment script:

python deploy.py

### ****Step 3: Open Jupyter Notebook****

Start Jupyter Lab:

jupyter lab

Then, navigate to the **"Model Stealing"** or **"Model Feature Extraction"** notebook and execute the cells one by one.

### ****Step 4: Test the Deployed Model****

To test the model, run:

python test\_model.py

### ****Step 5: Test the API****

To test the API, run:

python test\_api.py

### ****Step 6: Compare the Results****

Finally, compare the extracted model's performance with the original model and analyze the differences.