Smart Blocking at Scale: Defending Web Services from DDoS Attacks with AWS

This project is part of the Summer 2025 course COSC-6376-W01 Network Security. It demonstrates how to simulate a DDoS-style attack on a basic API and then defend it using AWS security tools like WAF (Web Application Firewall) and rate limiting.

# 📁 Project Structure

ddos-defense/  
├── app.py # Flask API  
├── requirements.txt # Python dependencies  
├── venv/ # Virtual environment (auto-created)  
└── README.docx # You're here!

# 🛠️ Getting Started

1. Open Your Terminal and Go to the Project Folder

cd "/mnt/data/School/Summer 2025/COSC-6376-W01 Network Security/ddos-defense"

2. Create a Virtual Environment

python3 -m venv venv

3. Activate the Virtual Environment

source venv/bin/activate

You should see (venv) in your terminal prompt now.

4. Install Required Packages

pip install -r requirements.txt

5. Run the Flask API

python3 app.py

Open your browser and visit: http://localhost:5000/api/hello

You should see: {"message": "Hello, world!"}

# 🧪 Next Steps

- Use Apache Benchmark (ab) or Locust to simulate a DDoS-style attack

- Deploy the app to AWS EC2 or another cloud platform

- Set up AWS WAF to monitor and block abusive traffic

- Log results and screenshots for your paper and presentation

# ⌨️ Stopping the App vs Exiting Virtual Environment

To stop the Flask app running: Press Ctrl+C in the terminal

To exit the virtual environment: Run the command "deactivate"

# 📚 Course Info

Course: COSC-6376-W01 Network Security

Semester: Summer 2025

Student: Daniel Hernandez

Project Title: Smart Blocking at Scale: Defending Web Services from DDoS Attacks with AWS