

**MICHIGAN STATE**  

---

**UNIVERSITY**

# Beta Presentation

## Hybrid Cyberattack Simulator

### The Capstone Experience

Team Vectra AI

Henry Barton

Alisha Brenholt

Nathan Motzny

Campbell Robertson

Andrew Talbott

Department of Computer Science and Engineering

Michigan State University

Spring 2024



*From Students...  
...to Professionals*

# Project Overview

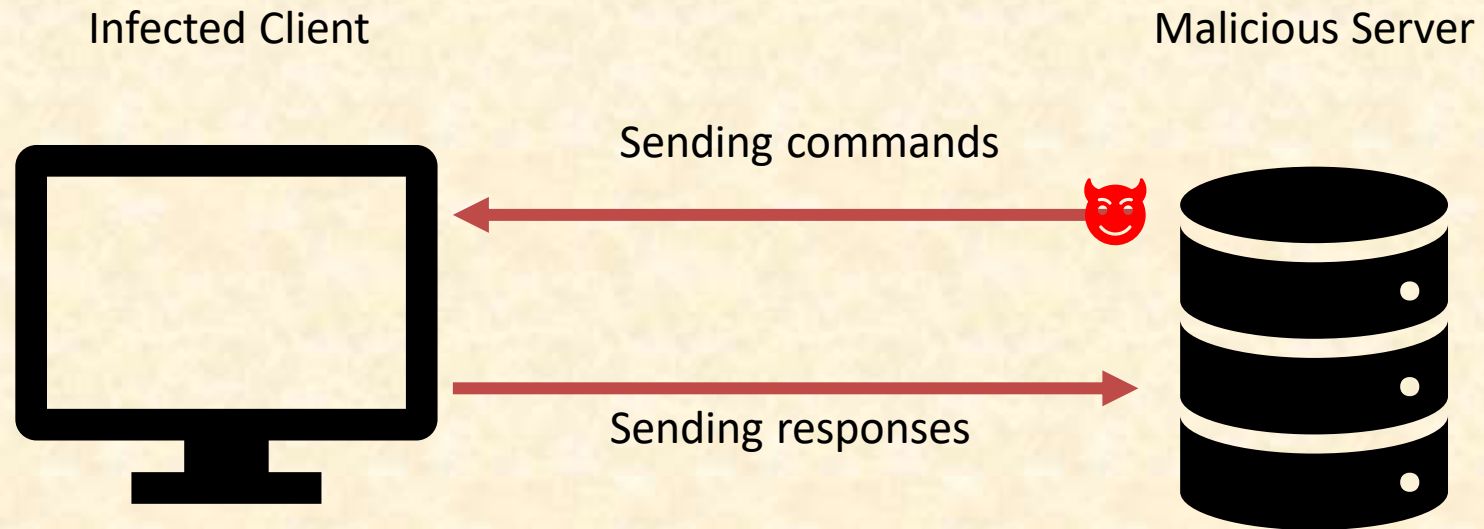
---

- **Problem:** Generating high quality, diverse, activity rich training data is not a problem that can be solved on a human scale
- **Solution:** Our software generates data at scale, including attacker activities which are essential to simulate real attacks

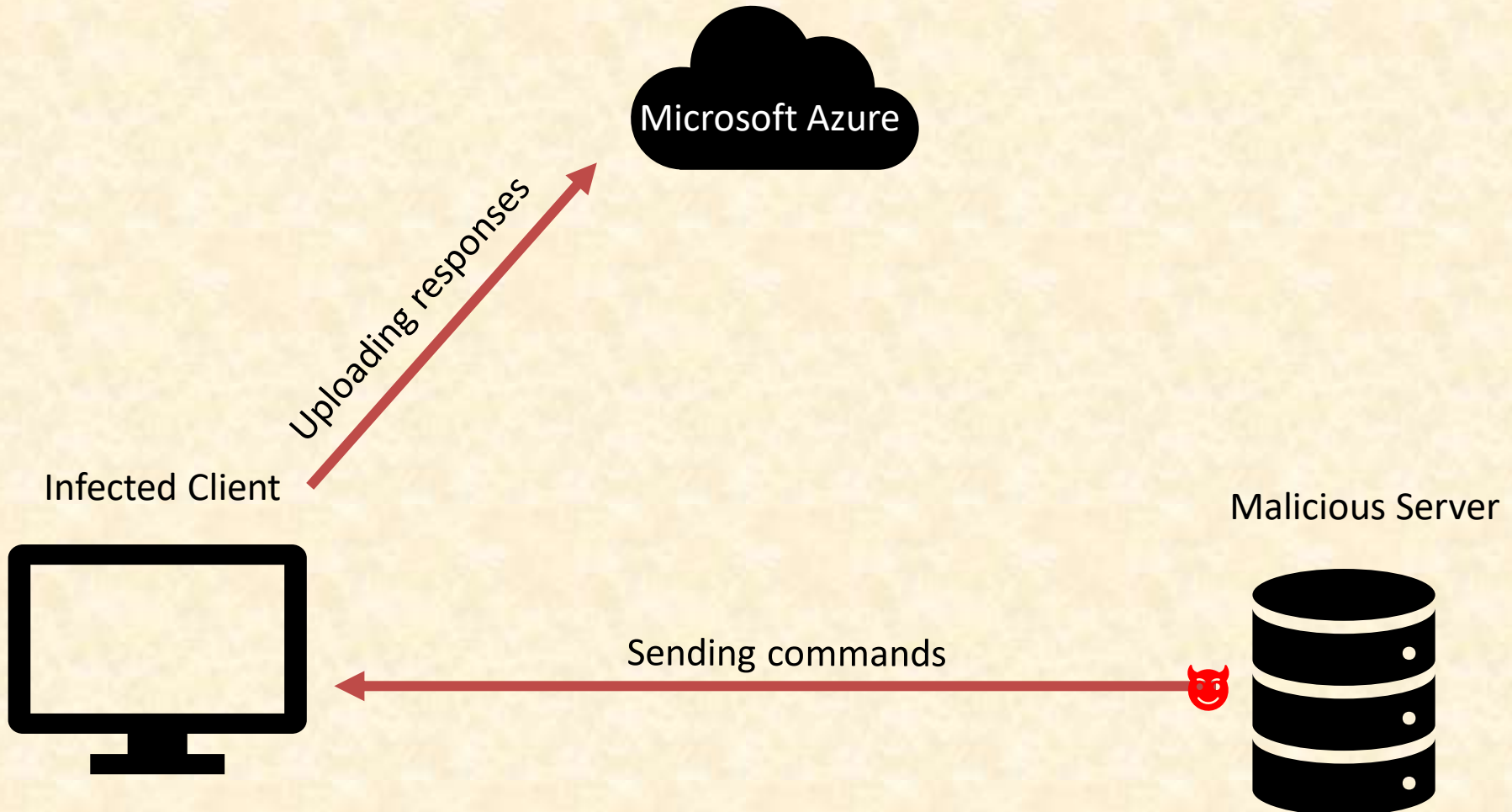
VECTRA®



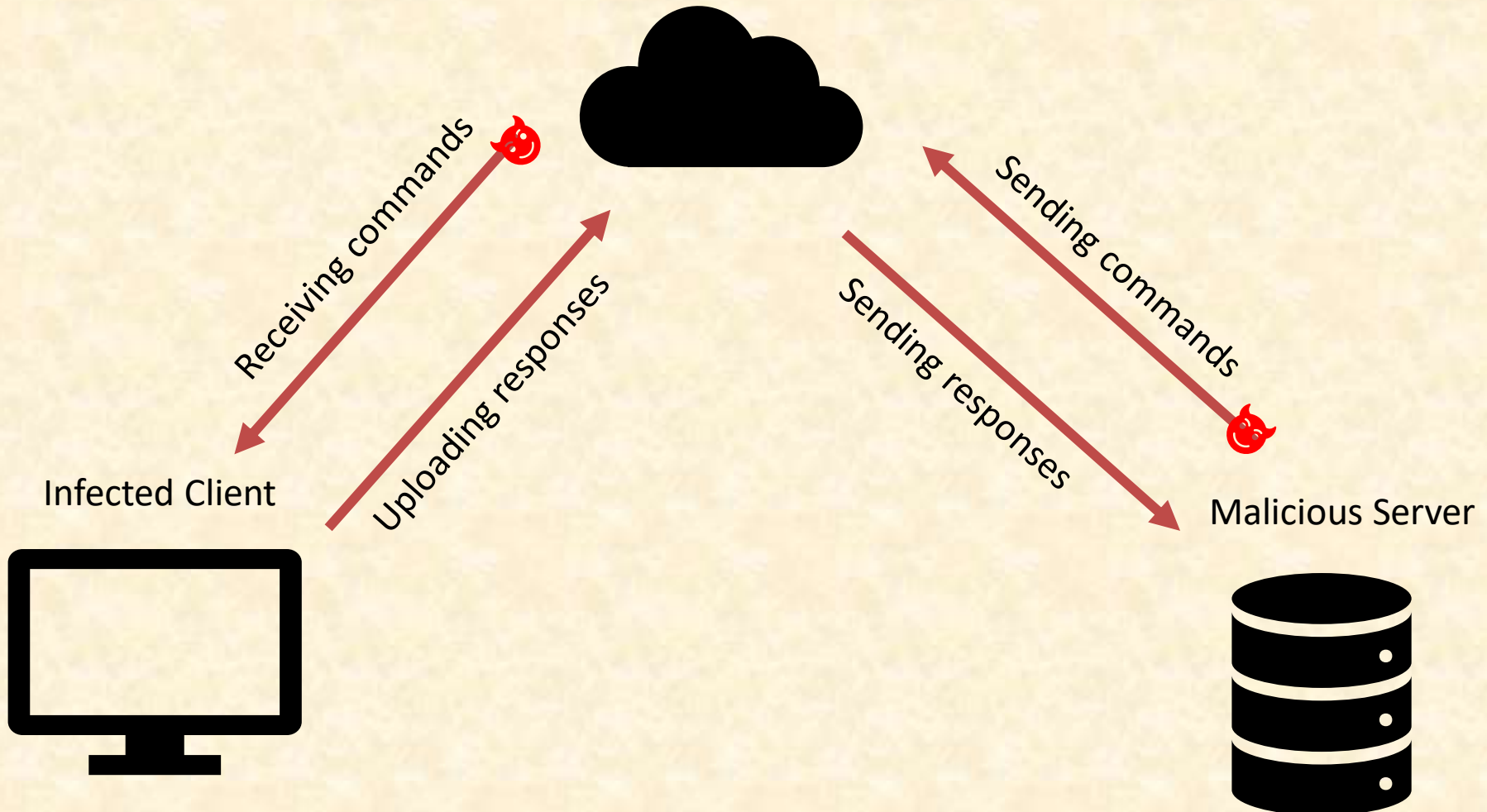
# Traditional Command and Control



# Hybrid Attack - MAAD

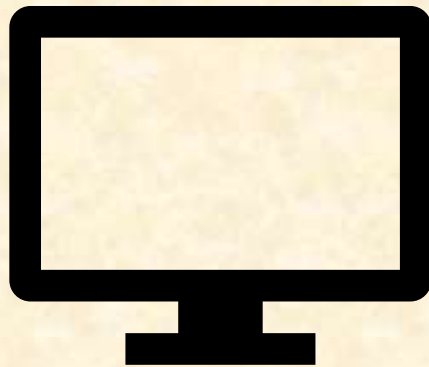


# REST API Attack

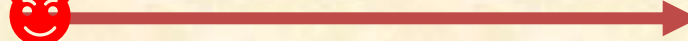


# Web Shell Attack

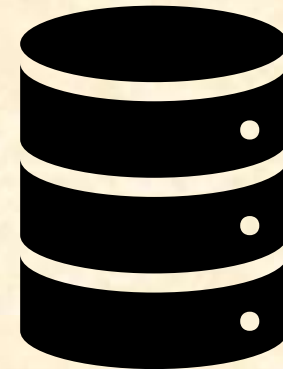
Malicious Client



Sending commands



Infected Server



Sending responses



# What's left to do?

---

- Features
- Stretch Goals
  - Run entirely on Web UI
- Other Tasks
  - Bug Fixes
  - Extensive Testing
  - Handling Edge Cases



# Questions?

---

?

?

?

?

?

?

?

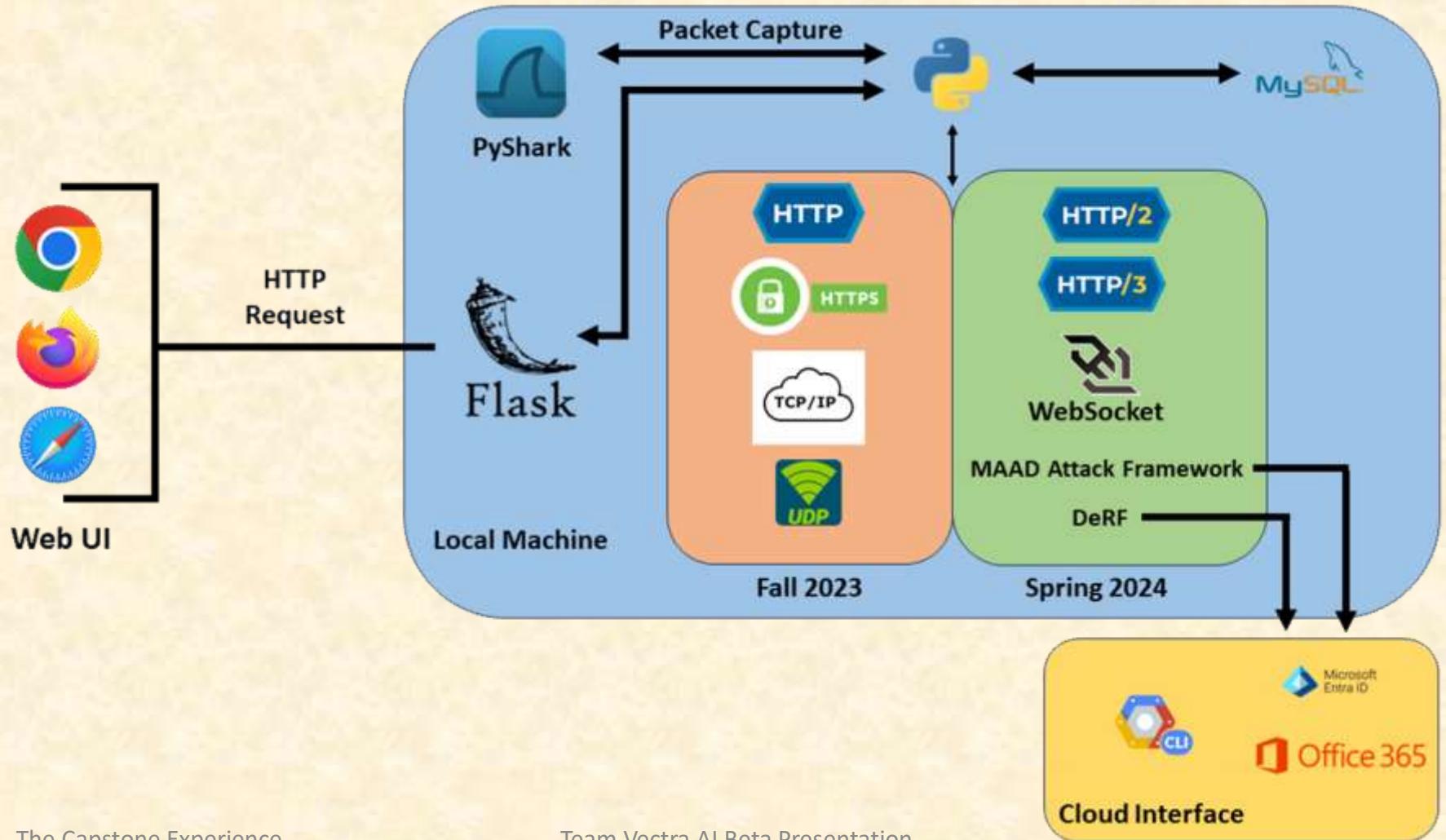
?

?





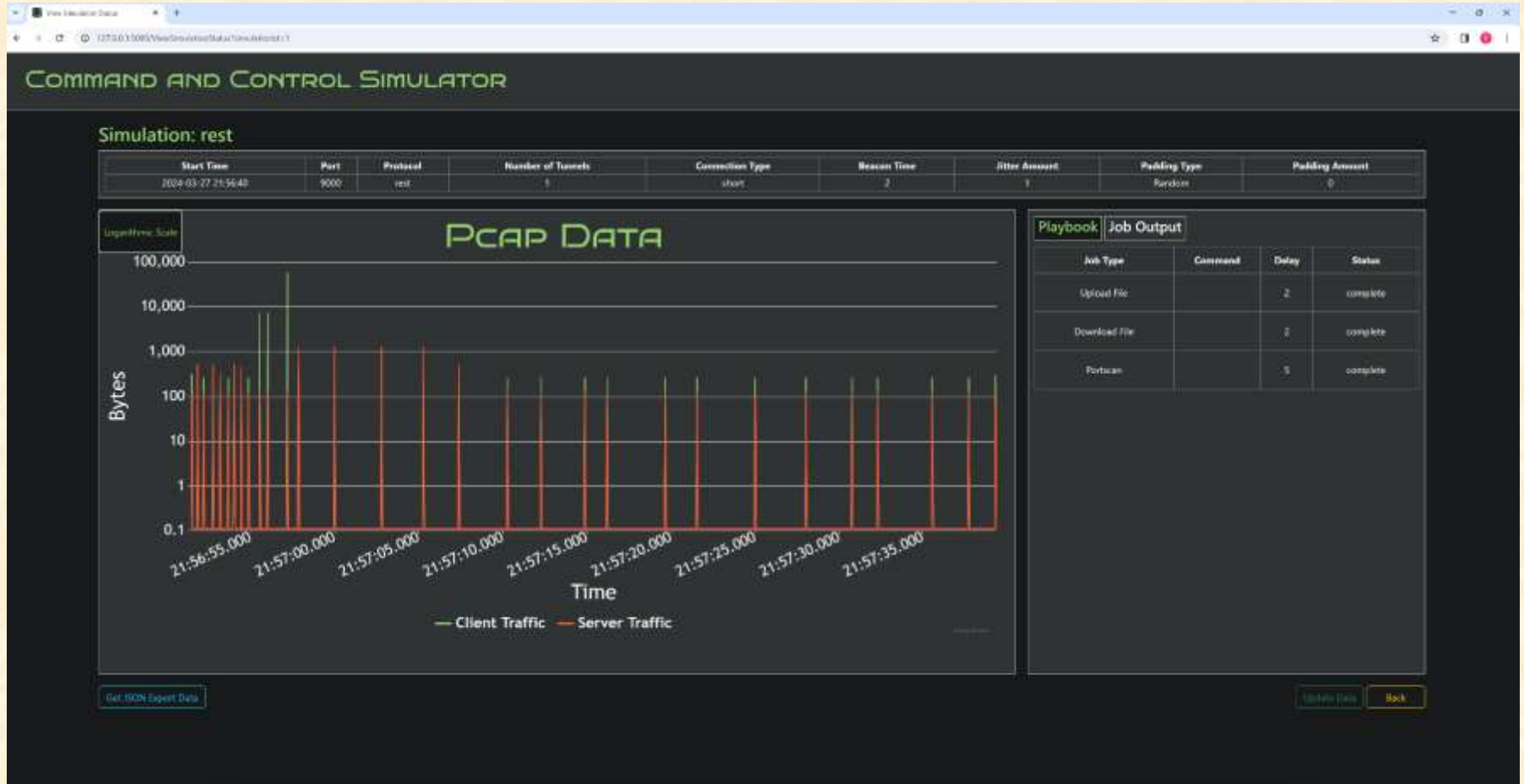
# System Architecture



# MAAD Attack Example



# REST API Attack



# Web Shell Attack Example



# Web Shell Examined More Closely

