MICHIGAN STATE
UNIVERSITY

# Beta Presentation
## Command & Control Simulator

## The Capstone Experience

### Team Vectra

Trevor Davis
Ben Hayes
Nixon Holley
Ben Tuckey
Andrew Vandercar

Department of Computer Science and Engineering
Michigan State University

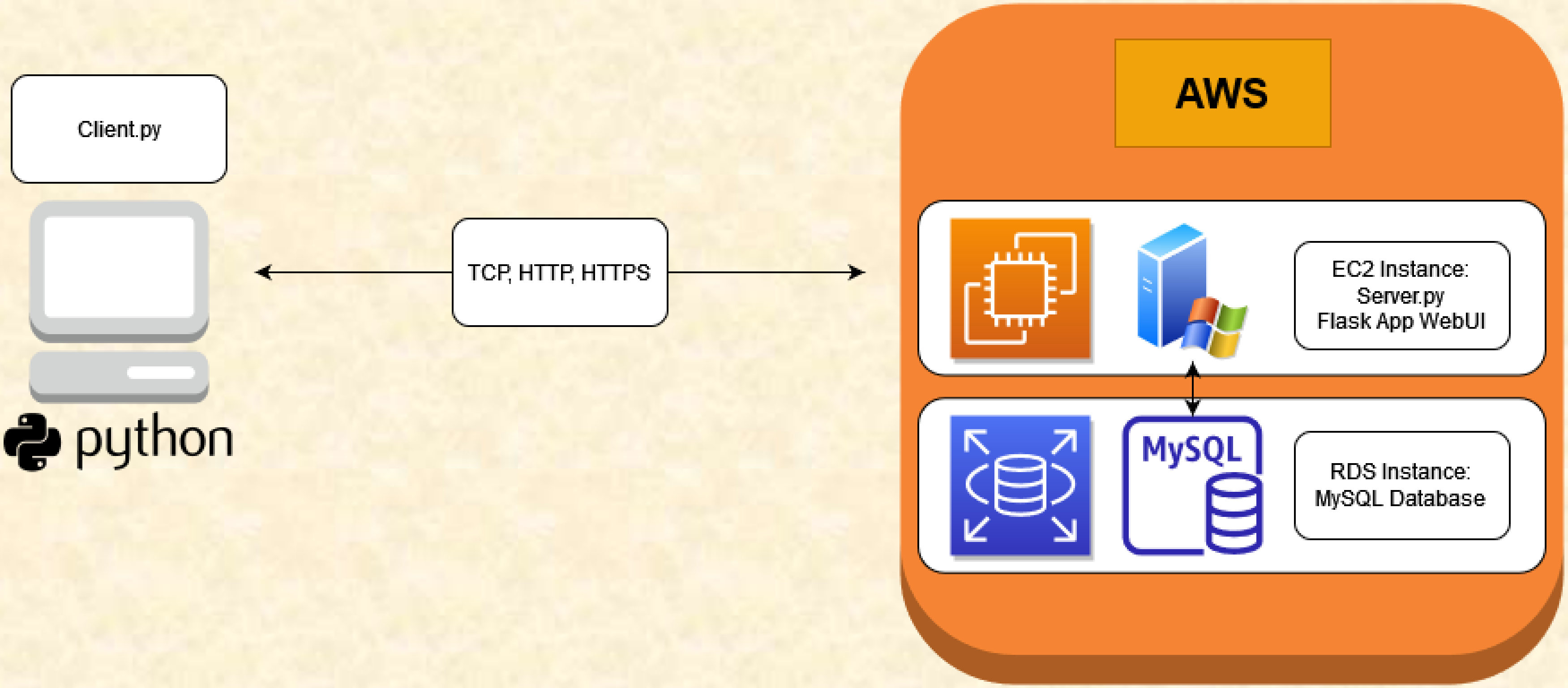
Fall 2023

*From Students…*
*…to Professionals*

# Project Overview

- C2 channels are used by attackers to control compromised devices
- Lack of public C2 data available to analysts
- Application simulates C2 channels
- Configurable parameters which replicate real-world attack behavior
- Log network traffic for data display/analysis
- Web UI controls the application and visualizes logs

# System Architecture



Client.py

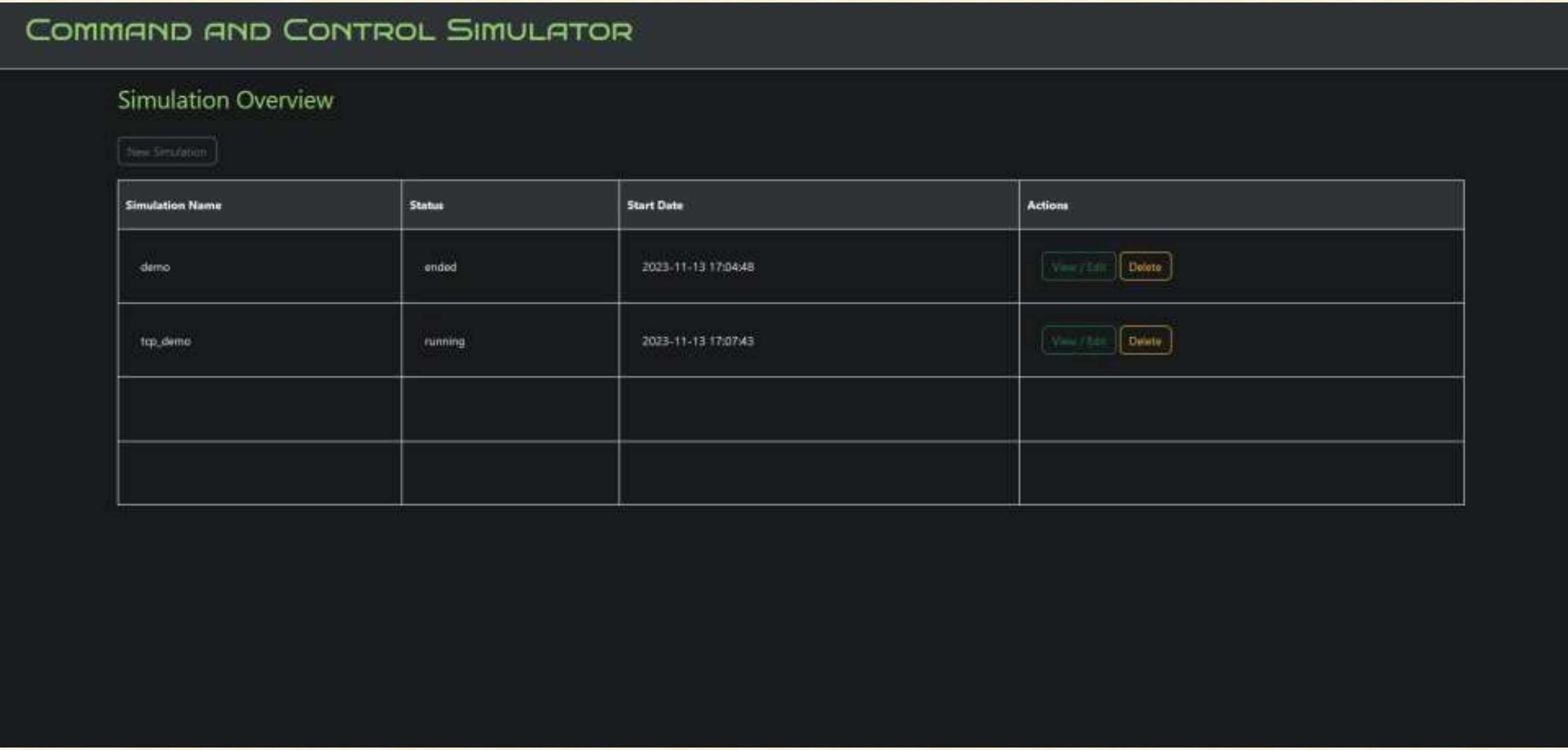
TCP, HTTP, HTTPS

AWS

EC2 Instance:
Server.py
Flask App WebUI

RDS Instance:
MySQL Database

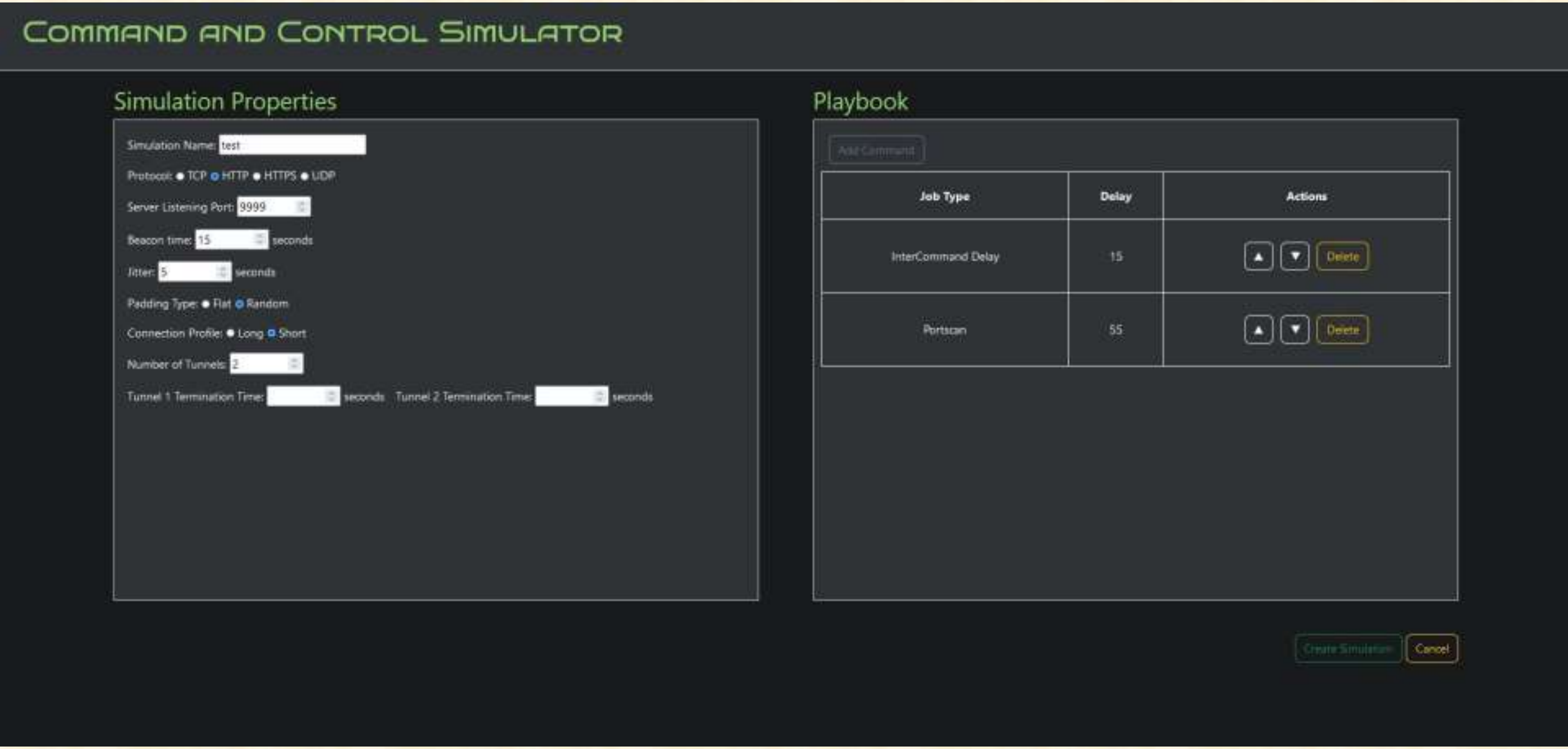
# Simulation Overview



Simulation Overview

| Simulation Name | Status | Start Date | Actions |
|---|---|---|---|
| demo | ended | 2023-11-13 17:04:48 | View / Edit Delete |
| tcp_demo | running | 2023-11-13 17:07:43 | View / Edit Delete |
| | | | |
| | | | |

# New Simulation



Command and Control Simulator

## Simulation Properties

Simulation Name: test

Protocol: ○ TCP ◉ HTTP ○ HTTPS ○ UDP

Server Listening Port: 9999

Beacon time: 15 seconds

Jitter: 5 seconds

Padding Type: ○ Flat ◉ Random

Connection Profile: ○ Long ◉ Short

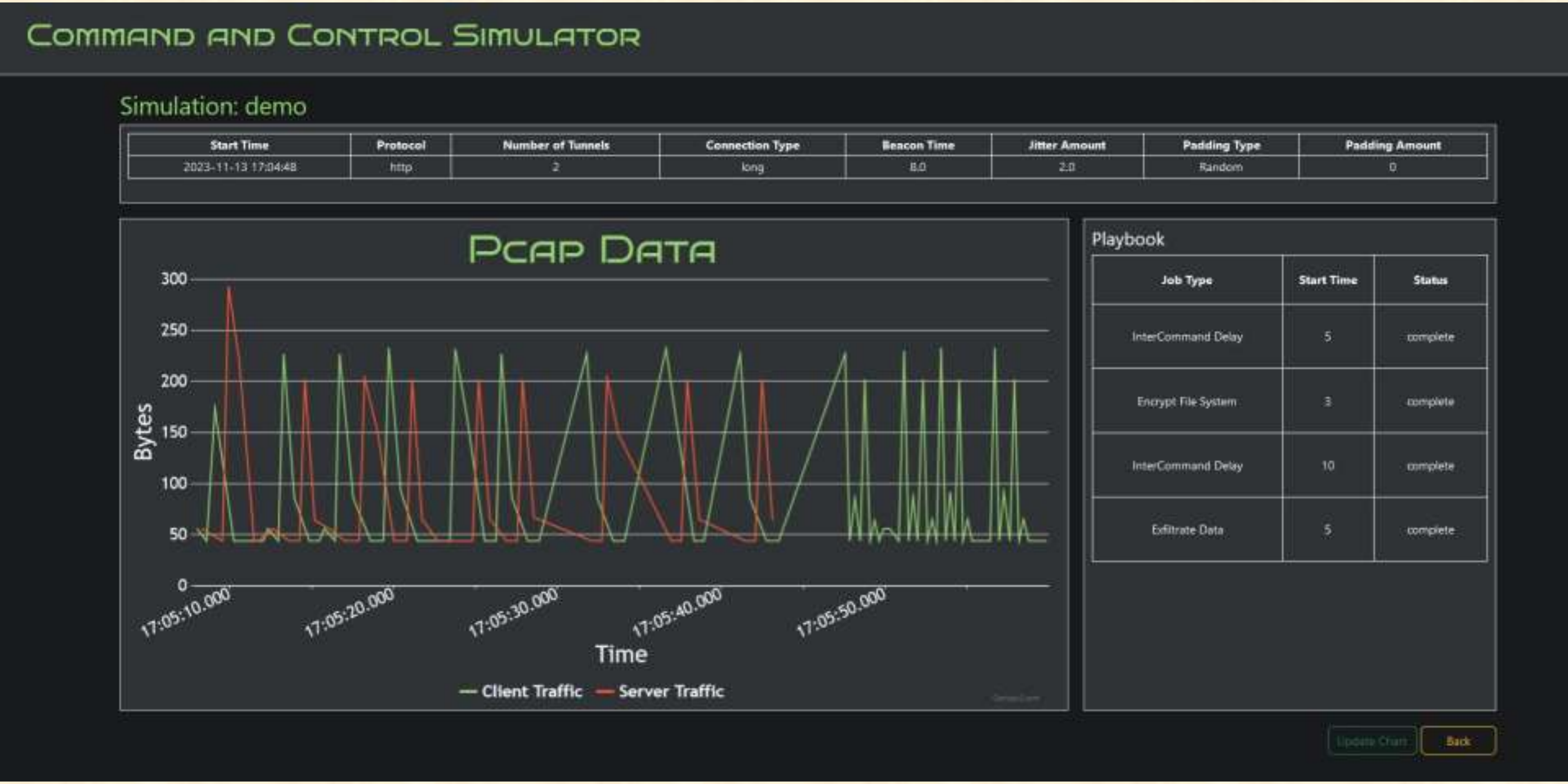
Number of Tunnels: 2

Tunnel 1 Termination Time: seconds Tunnel 2 Termination Time: seconds

## Playbook

| Job Type | Delay | Actions |
|---|---|---|
| InterCommand Delay | 15 | ▲ ▼ Delete |
| Portscan | 55 | ▲ ▼ Delete |

# Simulation Details



Simulation: demo

| Start Time | Protocol | Number of Tunnels | Connection Type | Beacon Time | Jitter Amount | Padding Type | Padding Amount |
|---|---|---|---|---|---|---|---|
| 2023-11-13 17:04:48 | http | 2 | long | 8.0 | 2.0 | Random | 0 |

Playbook

| Job Type | Start Time | Status |
|---|---|---|
| InterCommand Delay | 5 | complete |
| Encrypt File System | 3 | complete |
| InterCommand Delay | 10 | complete |
| Exfiltrate Data | 5 | complete |

# What’s left to do?

- Stretch Goals
  - HTTP versions 2 & 3
  - Remote shell mode
  - Clone simulation parameters
  - Automate running multiple simulations
- Other Tasks
  - Create software documentation
  - Refactor & Clean up code
  - Brainstorm additional features

# Questions?

? ? ? ?

? ?

? ? ?