From Students…
…to Professionals

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
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
Traditional Command and Control

Infected Client  Malicious Server

Sending commands

Sending responses
Hybrid Attack - MAAD
REST API Attack

Infected Client → Cloud → Malicious Server
- Receiving commands
- Uploading responses
- Sending responses
- Sending commands
Web Shell Attack

Malicious Client

Sending commands

Sending responses

Infected Server
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

Diagram showing the system architecture with components such as PyShark, Flask, Packet Capture, HTTP, HTTPS, TCP/IP, WebSocket, MAAD Attack Framework, DeRF, and Cloud Interface. The diagram also indicates local machine and projects spanning Fall 2023 and Spring 2024.
MAAD Attack Example
REST API Attack
Web Shell Attack Example
Web Shell Examined More Closely