MICHIGAN STATE UNIVERSITY

Alpha 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

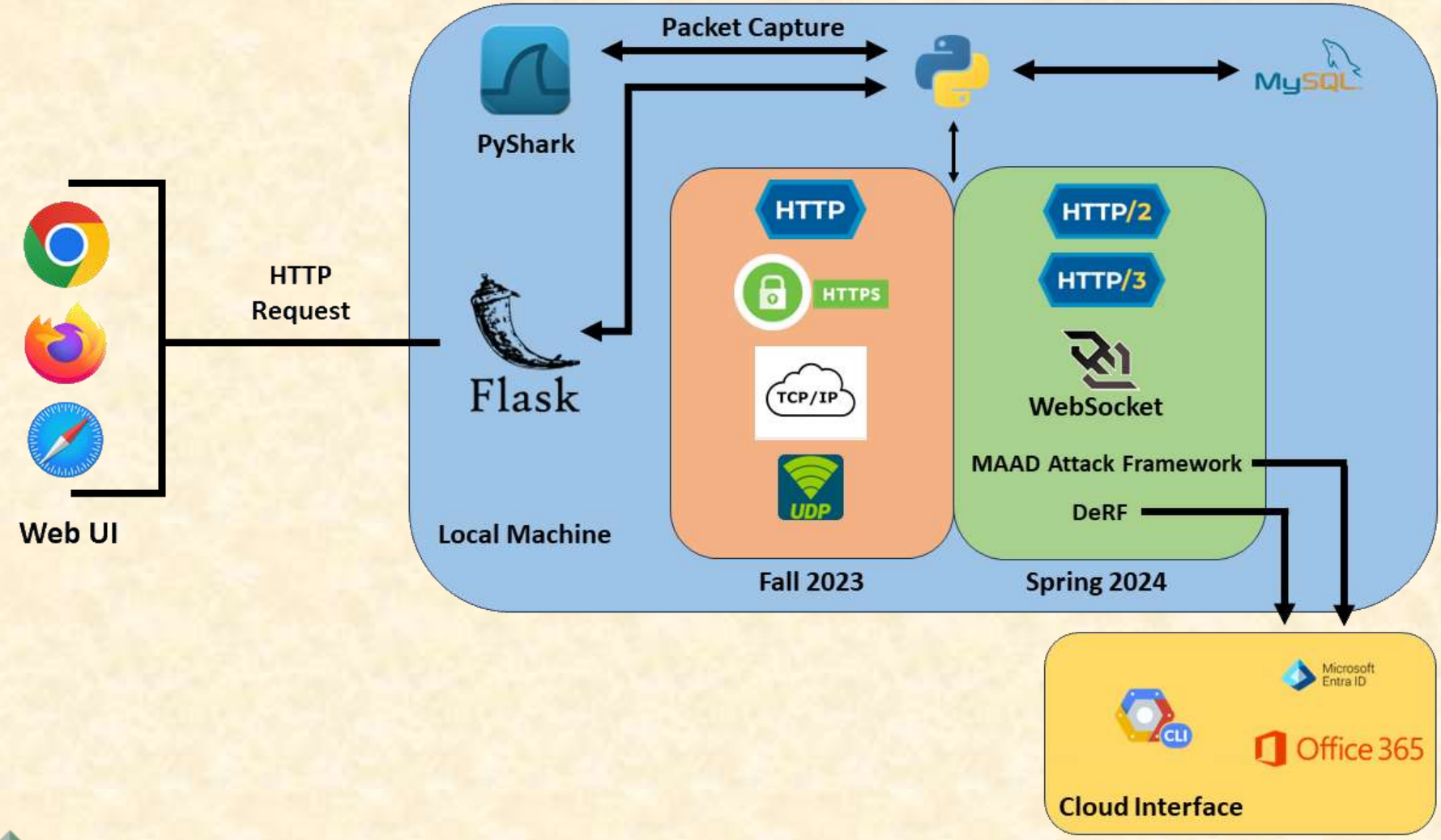
Spring 2024

From Students…
…to Professionals

Project Overview

- Vectra's AI models need relevant training data to maintain effectiveness
- Adding 3 new network protocols and advanced C2 configuration such as beaconless interaction and dynamic responses
- Also adding hybrid integration with third-party attack tools

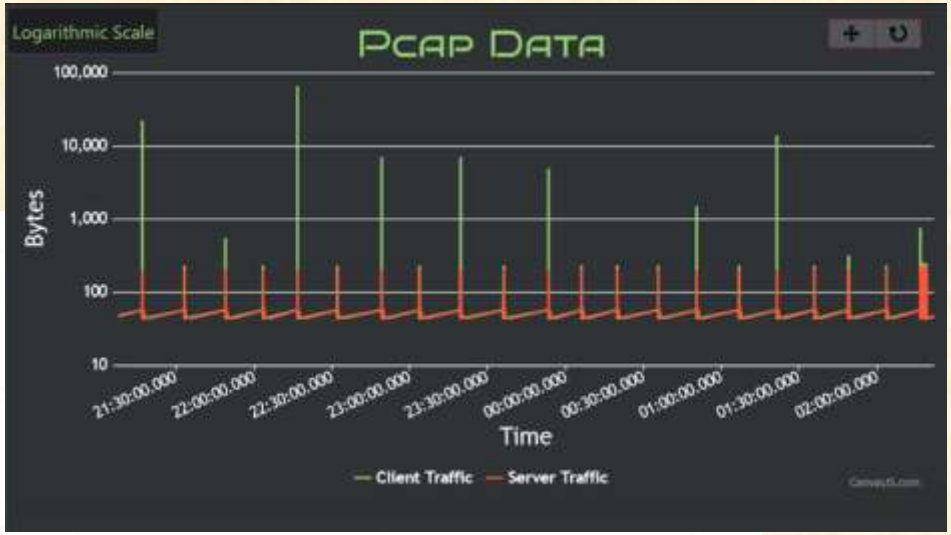
System Architecture

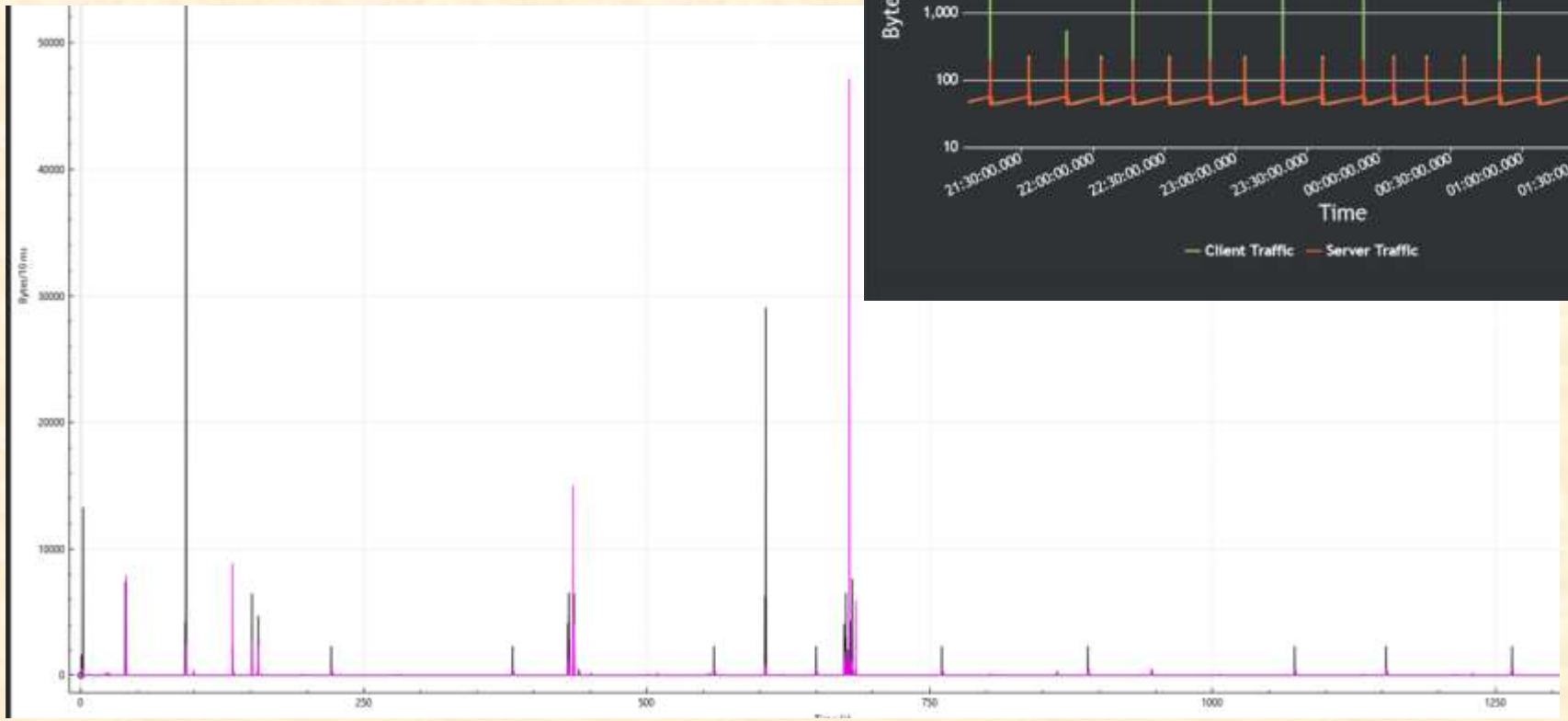


Project Risks

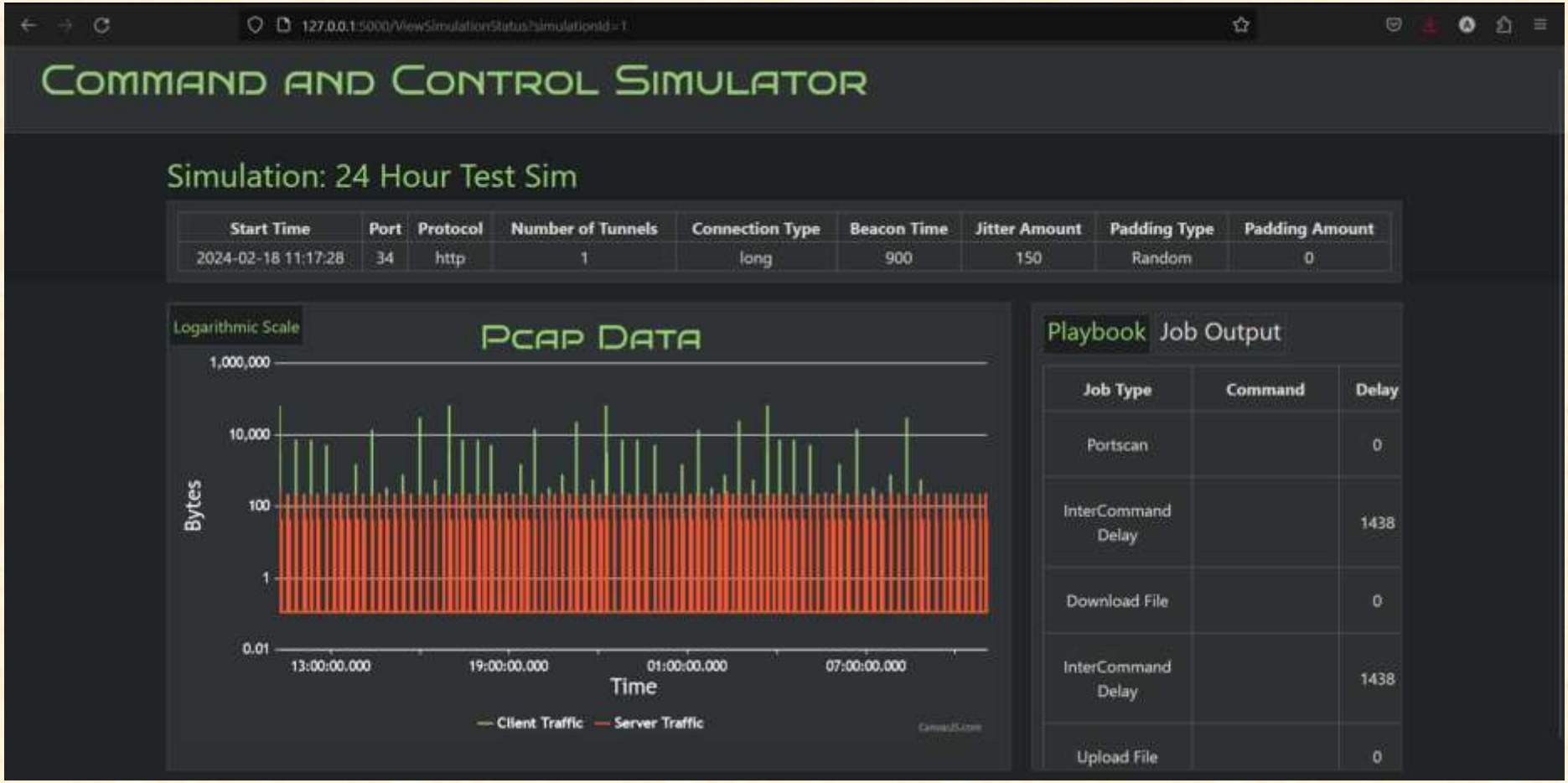
- Compatibility
  - Make sure all third-party apps work together
  - Using active libraries and using version control
- Generating Realistic Data
  - Generate realistic enough data for AI models to train on
  - Analyzing real world attacks and mimicking their outputs
- Performance Issues
  - Make large amounts of data in reasonable amounts of time
  - Spending time optimizing code; looking at distributed computing
- Portability
  - The program needs to be able to run on multiple OS without issue
  - Using cross-platform libraries and allowing API calls to server to abstract user operating system

Realistic Data versus Ours

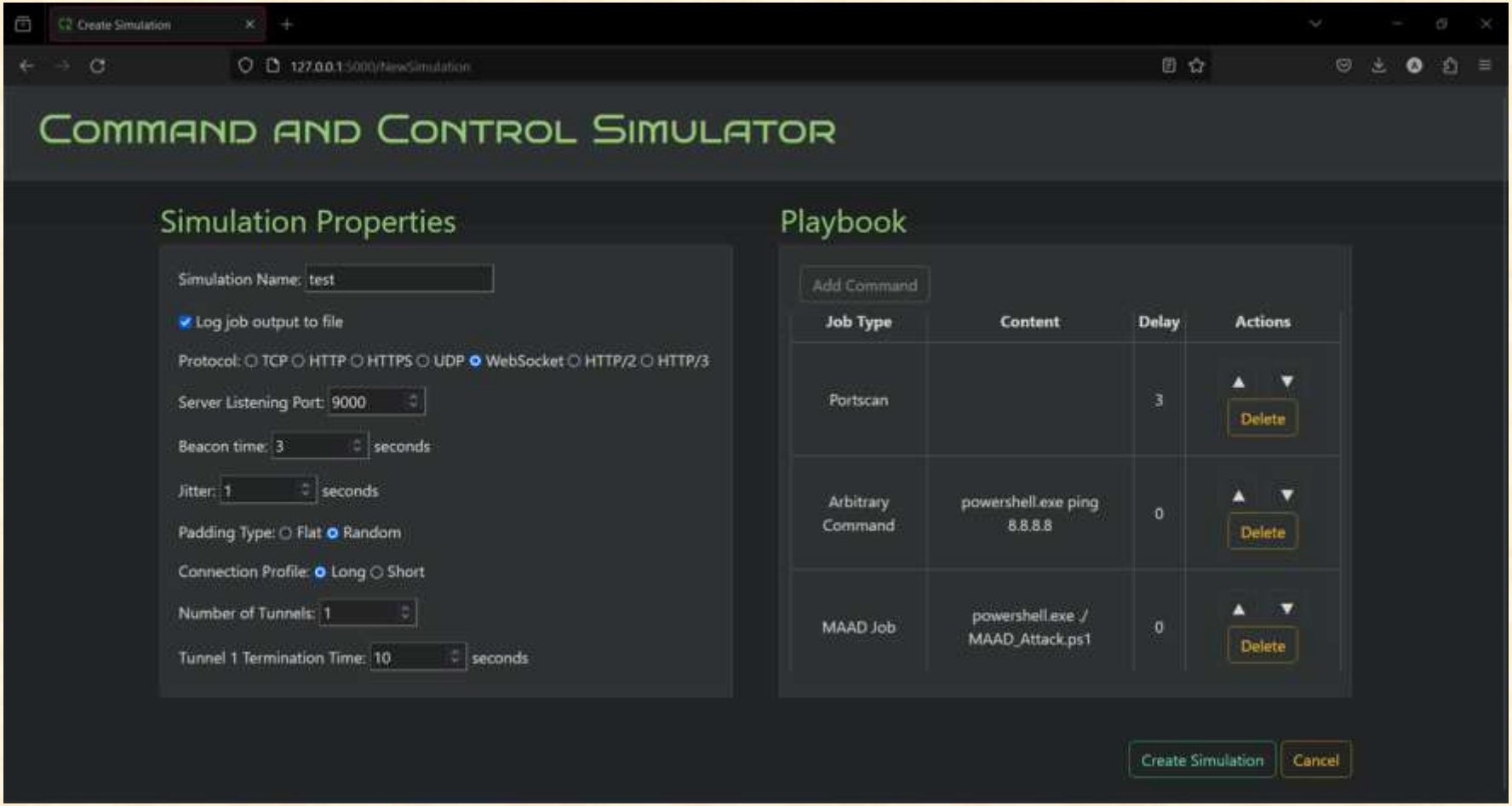




Result of 24 Hour Job



Configuring a WebSocket Job



The Client Terminal in Action

```
{'status': 'success'}
Job Result Successfully Sent to Server

Handling job Exfiltrate Data
Sending job response to server for job Exfiltrate Data
Connection is present
Connection<ConnectionKey(host='127.0.0.1', port=9000, is_ssl=False, ssl=None, proxy=None, proxy_auth=None, proxy_headers_hash=None)>
<ClientResponse(http://127.0.0.1:9000/job_result) [200 OK]>
<CIMultiDictProxy('Content-Type': 'application/json; charset=utf-8', 'Content-Length': '21', 'Date': 'Tue, 20 Feb 2024 00:46:04 GMT', 'Server': 'Python/3.12 aiohttp/3.9.1')>

Local address: 127.0.0.1, Local port: 63557
Beacon sent
{'status': 'success'}
Job Result Successfully Sent to Server

Handling job Encrypt File System
Sending job response to server for job Encrypt File System
Connection is present
Connection<ConnectionKey(host='127.0.0.1', port=9000, is_ssl=False, ssl=None, proxy=None, proxy_auth=None, proxy_headers_hash=None)>
<ClientResponse(http://127.0.0.1:9000/job_result) [200 OK]>
<CIMultiDictProxy('Content-Type': 'application/json; charset=utf-8', 'Content-Length': '21', 'Date': 'Tue, 20 Feb 2024 00:46:05 GMT', 'Server': 'Python/3.12 aiohttp/3.9.1')>

Local address: 127.0.0.1, Local port: 63557
Beacon sent
{'status': 'success'}
Job Result Successfully Sent to Server

Handling job Arbitrary Command
Files found, no need to download
b'\r\n'
b'Pinging 8.8.8.8 with 32 bytes of data:\r\n'
b'Reply from 8.8.8.8: bytes=32 time=14ms TTL=55\r\n'
b'Reply from 8.8.8.8: bytes=32 time=14ms TTL=55\r\n'
b'Reply from 8.8.8.8: bytes=32 time=15ms TTL=55\r\n'
b'Reply from 8.8.8.8: bytes=32 time=15ms TTL=55\r\n'
b'\r\n'
b'Ping statistics for 8.8.8.8:\r\n'
b'    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),\r\n'
b'Approximate round trip times in milli-seconds:\r\n'
b'    Minimum = 14ms, Maximum = 15ms, Average = 14ms\r\n'

Sending job response to server for job Arbitrary Command
Connection is present
Connection<ConnectionKey(host='127.0.0.1', port=9000, is_ssl=False, ssl=None, proxy=None, proxy_auth=None, proxy_headers_hash=None)>
<ClientResponse(http://127.0.0.1:9000/job_result) [200 OK]>
```

What’s left to do?

- Webshells
- REST API
- Malleable Profile
- HTTP/3
- Graph Job Start Times on Web UI

Questions?