

MICHIGAN STATE

UNIVERSITY

Alpha Presentation Command and 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
- Application simulates C2 channels
- Configurable parameters
- Log network traffic for data analysis
- Web UI controls the application and visualizes logs



Simulation Overview

Simulation Overview

New Simulation

Simulation Name	Status	Start Date	Actions
My simulation	Completed	11/11/2011 12:00AM	View / Edit Delete
My simulation 2	Completed	11/11/2011 12:00AM	View / Edit Delete



Create Simulation

COMMAND AND CONTROL SIMULATOR

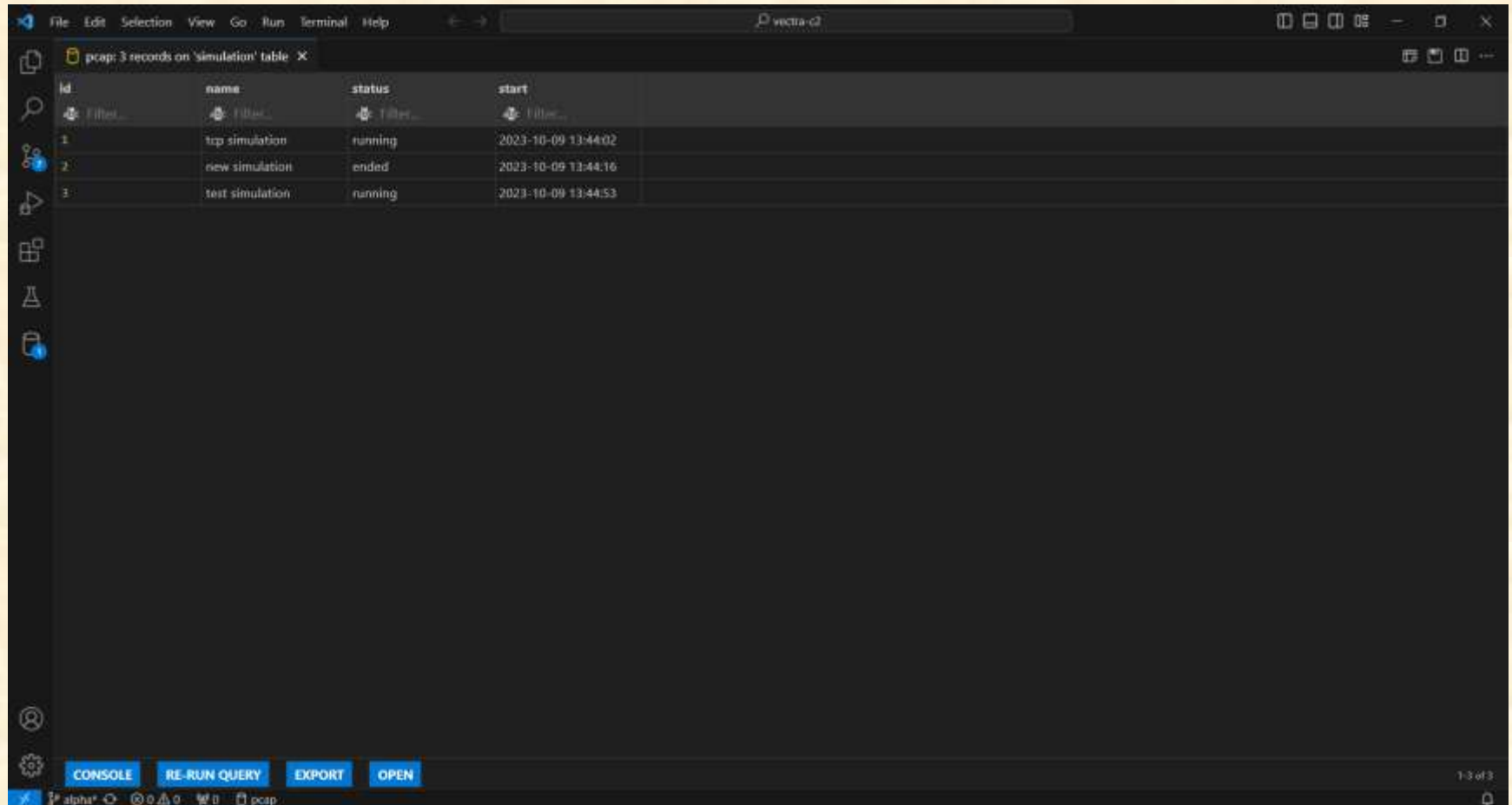
Create Simulation

New Simulation Name:

Tunnel Name	Protocol	Port Number	Jitter Range	Padding Range	Number of Commands	Actions
My tunnel	HTTP	8	5-30	13-50	4	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
My tunnel 2	TCP	2	6-10	16-30	2	<input type="button" value="Edit"/> <input type="button" value="Delete"/>



Database



The screenshot shows a database management interface with a table containing simulation records. The table has four columns: 'id', 'name', 'status', and 'start'. The data is as follows:

id	name	status	start
1	tcp simulation	running	2023-10-09 13:44:02
2	new simulation	ended	2023-10-09 13:44:16
3	test simulation	running	2023-10-09 13:44:53

The interface also includes a menu bar (File, Edit, Selection, View, Go, Run, Terminal, Help), a toolbar with various icons, and a bottom panel with buttons for 'CONSOLE', 'RE-RUN QUERY', 'EXPORT', and 'OPEN'. The status bar at the bottom shows 'alpha' and 'pcap'.



Terminal

```
tunnel.py  _init_.py X
WebsitePackage > _init_.py
?  from . import models
PROBLEMS  OUTPUT  DEBUG-CONSOLE  TERMINAL  PORTS

PS C:\Users\valab\Downloads\vectra-c2-alpha> python3 src/server.py
Traceback (most recent call last):
  File "C:\Users\valab\Downloads\vectra-c2-alpha\src\server.py", line 1
2, in <module>
    from aiohttp import web
ModuleNotFoundError: No module named 'aiohttp'
PS C:\Users\valab\Downloads\vectra-c2-alpha> python3 src/server.py

Serving on ("127.0.0.1", 9999)
Server listening for API on 127.0.0.1:9999

New Server Tunnel created. ID: 1

Sending Configuration File to Client at 127.0.0.1:56578

New Server Tunnel created. ID: 2

New Server Tunnel created. ID: 3
Received: beacon from client 127.0.0.1:56578
Queue Empty, No Jobs to Send

Received: beacon from client 127.0.0.1:56579
Queue Empty, No Jobs to Send

Received: beacon from client 127.0.0.1:56580
Queue Empty, No Jobs to Send

Server received request from api: {'api_code': 'execute_command', 'Simu
lationId': 1, 'Delay': 1, 'CommandType': 'portscan'}
Received: beacon from client 127.0.0.1:56578
Current Jobs Queued to Send: ['1,1,portscan']
Sending job 1,1,portscan

Server Received Confirmation of Job Completion From Client. Logging Job
Results: this is temporary return data for command portscan from tunne
l 1
[]

File "C:\Users\valab\Downloads\vectra-c2-alpha\WebsitePackage\main.py", line 1
, in <module>
    from WebsitePackage import create_web_app
File "C:\Users\valab\Downloads\vectra-c2-alpha\WebsitePackage\_
_init_.py", line 2, in <module>
    from . import models
File "C:\Users\valab\Downloads\vectra-c2-alpha\WebsitePackage\m
odels.py", line 4, in <module>
    import mysql.connector
ModuleNotFoundError: No module named 'mysql'
PS C:\Users\valab\Downloads\vectra-c2-alpha> python3 Website/main.py
Traceback (most recent call last):
  File "C:\Users\valab\Downloads\vectra-c2-alpha\Website/main.py", line 1
, in <module>
    from WebsitePackage import create_web_app
File "C:\Users\valab\Downloads\vectra-c2-alpha\WebsitePackage\_
_init_.py", line 2, in <module>
    from . import models
File "C:\Users\valab\Downloads\vectra-c2-alpha\WebsitePackage\m
odels.py", line 4, in <module>
    import mysql.connector
ModuleNotFoundError: No module named 'mysql'
PS C:\Users\valab\Downloads\vectra-c2-alpha> python3 Website/main.py
Connection error: 2003: Can't connect to MySQL server on 'localhost:338
6' (10001 No connection could be made because the target machine active
ly refused it)
Connection error: 2003: Can't connect to MySQL server on 'localhost:338
6' (10001 No connection could be made because the target machine active
ly refused it)
* Serving Flask app 'WebsitePackage'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production de
ployment. Use a production WSGI server instead.
* Running on http://127.0.0.1:5000
Press CTRL+C to quit
* Restarting with stat
Connection error: 2003: Can't connect to MySQL server on 'localhost:338
6' (10001 No connection could be made because the target machine active
ly refused it)
Connection error: 2003: Can't connect to MySQL server on 'localhost:338
6' (10001 No connection could be made because the target machine active
ly refused it)
* Debugger is active!
* Debugger PIN: 124-938-147
127.0.0.1 - - [09/Oct/2023 22:36:00] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Oct/2023 22:36:00] "GET /c2icon.ico HTTP/1.1" 200 -
Result from server: {'Result': 'Success'}
127.0.0.1 - - [09/Oct/2023 22:37:58] "POST /send_command HTTP/1.1" 200 -
[]

PS C:\Users\valab\Downloads\vectra-c2-alpha> python3 src/client.py 12
7.0.0.1 9999 tcp
Client Tunnel 1 created.
Client Tunnel 1 connected to Server

Configuration has been Received from Server and Parsed

Client Tunnel 2 created.
Client Tunnel 2 connected to Server

Client Tunnel 3 created.
Client Tunnel 3 connected to Server

Beacon (Size:100) Sent to Server 127.0.0.1:9999
No Jobs Received From Server.

Beacon Interval changed by 0.85 seconds

Beacon (Size:100) Sent to Server 127.0.0.1:9999
No Jobs Received From Server.

Beacon Interval changed by -0.00 seconds

Beacon (Size:100) Sent to Server 127.0.0.1:9999
No Jobs Received From Server.

Beacon Interval changed by 0.82 seconds

Beacon (Size:100) Sent to Server 127.0.0.1:9999
Received Job On Tunnel 1: PORTSCAN (Delay: 1 seconds) (
Size: 12)
Beacon Interval changed by 0.81 seconds

Tunnel 1 Executed Command PORTSCAN After Delaying 1.0 Seconds
[]

Ln 2, Col 1  Space:4  UTF-8  LF  Python  Q
```

What's left to do?

- Add HTTP/HTTPS protocols
- Add “View Simulation” page on the Web UI
- Get the Web UI to display data from the MySQL server
- Set up MySQL server on AWS
- Add tunnel termination time parameter
- Configure command handling behavior



Questions?

?

?

?

?

?

?

?

?

