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
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

**Command and Control Simulator**

<table>
<thead>
<tr>
<th>Simulation Name</th>
<th>Status</th>
<th>Start Date</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>My simulation</td>
<td>Completed</td>
<td>11/11/2011 12:00AM</td>
<td>View / Edit, Delete</td>
</tr>
<tr>
<td>My simulation 2</td>
<td>Completed</td>
<td>11/11/2011 12:00AM</td>
<td>View / Edit, Delete</td>
</tr>
</tbody>
</table>
Create Simulation

Command and Control Simulator

Create Simulation

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Protocol</th>
<th>Port Number</th>
<th>Jitter Range</th>
<th>Padding Range</th>
<th>Number of Commands</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>My tunnel</td>
<td>HTTP</td>
<td>8</td>
<td>5-30</td>
<td>13-50</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>My tunnel 2</td>
<td>TCP</td>
<td>2</td>
<td>6-10</td>
<td>16-30</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
Database
Terminal
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?