EDURange: Meeting the Pedagogical Challenges of Student Participation in Cybertraining Environments

Stefan Boesen (Dartmouth College)
Richard Weiss (The Evergreen State College)
Michael Locasto (The University of Calgary)
James Sullivan (The University of Calgary)
Jens Mache (Lewis & Clark College)
Erik Nilsen (Lewis & Clark College)

Supported by grants from the National Science Foundation NSF DUE 1141341 and 1141314 and Amazon
Motivation for Building EDURange

Existing testbeds have certain limitations...

As instructors, we were looking for:

- flexibility
- scalability
- analysis skills
Analysis Skills

• Verify Assumptions using network messages, error messages, system calls, static analysis
• Matching actual system behavior with predicted behavior
• Extracting information from opaque artifacts
• Creating resilience based on understanding failure modes
The EDURange Architecture

Hosted on EC2

Minimal “client” requirements

Currently 6 scenarios (reconnaissance, binary analysis, network topology discovery, ...)

8/18/14 4 EDURange Project
## EDURange Events/Workshops

<table>
<thead>
<tr>
<th>When</th>
<th>Where/What</th>
<th># of people</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2013</td>
<td>SISMAT</td>
<td>12</td>
</tr>
<tr>
<td>Aug 2013</td>
<td>EDURange Internal Hackathon I</td>
<td>11</td>
</tr>
<tr>
<td>Oct 2013</td>
<td>CCSC-NW</td>
<td>8 faculty</td>
</tr>
<tr>
<td>Nov 2013</td>
<td>Evergreen Network Security course</td>
<td>40</td>
</tr>
<tr>
<td>Jan 2014</td>
<td>MPICT</td>
<td>7 faculty</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>L&amp;C Cybersecurity course</td>
<td>19</td>
</tr>
<tr>
<td>Feb 2014</td>
<td>UofC graduate seminar</td>
<td>4</td>
</tr>
<tr>
<td>March 2014</td>
<td>UofC Network Security course</td>
<td>25</td>
</tr>
<tr>
<td>March 2014</td>
<td>SIGCSE workshop</td>
<td>14 faculty</td>
</tr>
<tr>
<td>May 2014</td>
<td>EDURange Internal Hackathon II</td>
<td>15</td>
</tr>
<tr>
<td>June 2014</td>
<td>SISMAT 2014</td>
<td>17</td>
</tr>
</tbody>
</table>
Types of Exercises

• Reconnaissance: finding hosts with open ports on a complex network
• Fuzzing a calculator
• Crafting packets to find data on a hidden host
• Analyzing system calls by an unknown process
• Finding malware within a linkable file format
Lessons Learned

Techno-pedagogical challenges
Students need significant scaffolding
No client software to install, but distributing credentials was a speed bump
Faculty want exercises they can use right away

Everyone is proposing a cybertraining environment, why is this task more subtle than many anticipate?
Where to get it

• http://github.com/edurange/
• http://edurange.org/