Collaborative Penetration Testing
With Lair
About Us

• Tom Steele
  – Consultant at FishNet Security
  – @_tomsteele

• Dan Kottmann
  – Consultant at FishNet Security
  – Security assessments
  – Hobbyist coder
  – @djkottmann
The Problem
## Lair

Table with columns: IP Address, Hostname, Operating System, Last Update By.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
<th>Operating System</th>
<th>Last Update By</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.4</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.5</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.6</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.46</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
<tr>
<td>192.168.1.167</td>
<td>unknown</td>
<td>nmap</td>
<td>nmap</td>
</tr>
</tbody>
</table>

Lair 0.1.2 development lead by FishNet Security
What is Lair

• Web application for managing and tracking the execution of network assessments
• Simplifies effort needed to execute a comprehensive, systematic pentest
• Open-source project sponsored by FishNet Security
• Imports, aggregates, and normalizes output from automated tools
Why is it different?

• Updates pushed to distributed testers in near real-time (really real-time, no really)
  – Reduces duplication of effort
    • Workflow
    • Status tracking
  – Enhances information sharing
    • Credentials/hashes found
    • Manually identified vulnerabilities
    • Successful exploitation
    • False positives
    • Screenshots
  – Team Instant Messaging
Technology

• Web application built on Node.js and Meteor
  – Simplifies real-time synchronization of information across multiple, distributed clients
  – Pub/sub concept
  – No need to fight web sockets
• Python used for Drones
• Mongodb used for database backend
Architecture
Long Demo Now
Download it

https://bitbucket.org/fnsseca/lair