Cybersecurity Assurance Program (CAP)

Red Team

May 2012
Importance of Red Teaming

- Challenge Organizational Thinking
- Unbiased view of network defense and security
- More realistic picture of security readiness than
  - Exercises
  - Role playing
  - Announced Assessments
Traditional Red Teaming

- Incorporates testing the organization’s:
  - Intelligence of the organization’s threat
  - Physical Security (e.g., locks, physical access to network, dumpster diving)
  - Institutional Posture (e.g., SOPs, Policies)
  - Network Security (e.g., vulnerabilities)

- Can suffer from “Target Fixation”

- Guaranteed maximum effort with potential for minimal return
Our Red/Blue Team Approach

• Collaborate with the agency to optimize engagement ROI for the Agency
  • Identify high priority targets
  • Streamlined “Attack” Process
  • Emphasize Risk Based Mitigation

• Utilize multiple enterprise class tools

• Leverage team expertise

• Validates the integration of People, Process, and Technology
Building a Bigger Picture

• Vulnerability and risk data gathered through Red Teaming will be non-attributable (stripped of any identifiers connected to specific agencies)

• Non-attributable data will then be aggregated and analyzed as a whole to reveal government-wide trends and most pressing vulnerabilities

• Aggregate data will be leveraged to benefit the entire Federal cybersecurity community
Future Opportunities

• Leveraging results for specific, actionable outreach projects

• Establishing an information exchange for Federal cybersecurity practitioners

• Address trending issues with immediate responses and mitigation tactics through a vulnerability and threat-specific help desk or hotline

• Providing guidance to organizations on establishing internal Red Teaming activities
Case Study: RVA Assessment #1

- **Main Test:** Web Application
- Accessed through a SSL-VPN connection
- A few issues were identified with the Web Application
- Main issue turned out to be the SSL-VPN connection
- While watching the traffic to and from the Web Application, we were able to:
  - It was *manual* testing that revealed the major problems
- **Agency Actions:** Immediately reviewed finding and remediated issue within 1 day. Requested additional testing to validate remediation, as assessment testing was still in progress.
Case Study: RVA Assessment #2

- **Main Test:** Web Application
- Scanner picked up a few issues with Web Application
- Main issue with Web Application was identified by watching the traffic and noticing that the cookies were the same for all users and could use this information to:
  - Elevate privileges from user to administrator
  - Gain access to any administrator account (over 45 different administrator accounts for over 45 different agencies)
- Could obtain access to personnel information
- It was **manual** testing that revealed the major problems
- **Agency Actions:** Agency worked with RVA team during test phase to develop remediation strategies. Critical finding strategies deployed within a few weeks and RVA team requested to retest. Lower priority items addressed within a few months.
Case Study: RVA Assessment #3

- Main Test: Most services were requested
- Social Engineering
  - 16% success rate with phishing emails
- Internal Scan revealed:
  - Unpatched systems & weak credentials to access Database (DB)
    - Identified user and passwords in DB
    - DB contained PII (Note: testing stopped on DB – the adversary would not have stopped)
- Piecing together findings, it would be relatively easy for an adversary to obtain access to critical systems through phishing
- Agency Actions: Agency was provided details of critical findings during assessment for their review and development of remediation plans.
## CM & RT/BT: Complementary, Not Exclusive

<table>
<thead>
<tr>
<th>CM</th>
<th>RT/BT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assist in getting results faster</td>
<td>• Determine if vulnerabilities are exploitable</td>
</tr>
<tr>
<td>• Identify weaknesses in scanned assets</td>
<td>• Conduct interviews to understand customer’s network</td>
</tr>
<tr>
<td>• Scan</td>
<td>• Correlate business risk to vulnerability rankings</td>
</tr>
<tr>
<td>• Web Applications</td>
<td>• Identify</td>
</tr>
<tr>
<td>• Database(s)</td>
<td>• human weaknesses, to include social engineering risks</td>
</tr>
<tr>
<td>• Operating Systems</td>
<td>• Logic Flaws</td>
</tr>
<tr>
<td>• Network Devices</td>
<td>• Configuration Issues</td>
</tr>
<tr>
<td>• Passive in nature</td>
<td>• Compound security issues</td>
</tr>
<tr>
<td></td>
<td>• Passive and Active in nature</td>
</tr>
</tbody>
</table>