A Graph-Theoretic Visualization Approach To Network Risk Analysis

Kenneth Prole
Scott O’Hare, Ph.D.
Applied Visions, Inc., Secure Decisions division

Steven Noel, Ph.D.
Center for Secure Information Systems
George Mason University

VizSec 2008
MIT - Cambridge, MA
September 15, 2008
Introduction

- Topological Vulnerability Analysis (TVA) attack graph technology
  - Builds comprehensive input model from network scans and database of potential attacker exploits
  - Analyzes vulnerability dependencies and models attack paths into a network
  - Discovers attack paths that convey the impact of individual and combined vulnerabilities on overall security

- New visualization approach
  - Dynamic interlinked views with high-level overview and detail drilldown
Architecture

Known Threats

Vulnerability Scans

Asset Discovery

Network Attack Model

What-If

Network Hardening

Visualization
## Evolution Stage 1: Single Attack Paths

<table>
<thead>
<tr>
<th>Step</th>
<th>Exploit</th>
<th>Attacker</th>
<th>Middleman</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>arp_flood</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>2</td>
<td>sniff_ypdom</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>3</td>
<td>conn_ypdom</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>4</td>
<td>ypcat_passwd</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>5</td>
<td>crack_passwd</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>6</td>
<td>scp_upload_pw</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>7</td>
<td>ssh_login_pw</td>
<td>attack</td>
<td></td>
<td>bart</td>
</tr>
<tr>
<td>8</td>
<td>rh62_glibc_bof</td>
<td>bart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>create_nfs_home_ssh_pk_su</td>
<td>bart</td>
<td></td>
<td>homer</td>
</tr>
<tr>
<td>10</td>
<td>ssh_login_pk_su</td>
<td>bart</td>
<td></td>
<td>homer</td>
</tr>
</tbody>
</table>
Evolution Stage 2: All Paths
Evolution Stage 3: Graph Aggregation
Evolution Stage 4: Interactive Visualization
Next Evolution in Attack Graph Visual Analysis

Overview Pane

Tree View

Graph View

Harden List

Exploit Table

Exploit Field

Defense

Graph View

Toolbars