Firewall Testing

Dr. E. Eugene Schultz, Prof. Sonia Fahmy, Florian Kerschbaum, Manu Pathak, Hao Wu, Mike Frantzen, Eric Hlutke, Seny Kamara
Motivation

• Current firewall testing based only on known vulnerabilities
• Firewall models lack detailed descriptions
• No prediction about potential vulnerabilities
Model

• Based on a data flow model
• Details firewall functionality
• Flexible to model different implementations
• Provides basis for analysis and prediction
Vulnerability Classification

• Analysis of known vulnerabilities
• Categorization into software vulnerabilities: Ivan Krsul’s Ph.D. thesis
• Mapping to data flow model
Vulnerability Categories

• memavail: Assumes that enough memory is available
• netdata: Assumes that network data is valid and bounded
• reassembly: Assumes that reassembly does not change data
• insufverif: Assumes that a set of verifications is sufficient
• trustnetobj: Assumes that network data can be trusted
• criticalsect: Assumes protection of critical section is sufficient
Future Work

• continue vulnerability classification
• predict vulnerabilities based on analysis
• test predicted vulnerabilities
• improve firewall model for possible attacks
Packet Ingress
NAT/PAT
Dynamic Rule Set
Sanity Checks
Port Filtering
Packet Reassembly
Application Level
Routing Decision
NAT/PAT
Address Lookup
Packet Egress

Packet may be dropped
Stream may be dropped

Bypass on
Match
<table>
<thead>
<tr>
<th>Software Flaw</th>
<th>Data Model</th>
<th>NAT/PAT</th>
<th>Dynamic Rule Set</th>
<th>Sanity Checks</th>
<th>Port Filtering</th>
<th>Packet Reassembly</th>
<th>Application Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>memavail</td>
<td></td>
<td></td>
<td>FW-1 ACK Saturation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>netdata</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PIX Frag. DOS</td>
<td>FW-1 Script Tag</td>
</tr>
<tr>
<td>reassembly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fragmented SYN</td>
<td>FTP PASV</td>
</tr>
<tr>
<td>insufverif</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Raptor ICMP</td>
<td></td>
</tr>
<tr>
<td>trustnetobj</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Int. address forwarded</td>
<td></td>
</tr>
<tr>
<td>criticalsect</td>
<td></td>
<td></td>
<td>FW-1 NAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>