Systems and Network Security Midterm Exam

Date: 18.06.2009  
Duration: 120 Mins.

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q5</th>
<th>Q6</th>
<th>Q7</th>
<th>Q8</th>
<th>Q9</th>
<th>Q10</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>15</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>35</td>
<td>10</td>
<td></td>
<td>125 pts</td>
</tr>
</tbody>
</table>

Questions

1) “All of the new security technologies coming out total a one or two order of magnitude increase in an attacker's costs. That's not impossible, that's just inflation. So deal.” - Dave Aitel

Please explain the statement above. What can you say about economics of cybercrime? (10 Pts.)

2) Please explain the interrupt descriptor table (IDT) and the system service dispatch table (SSDT). Can a user mode rootkit running with a low privileged user account modify these tables? Please support your arguments. (15 Pts.)

3) What is the difference between IDP and IDS? Which one would you recommend to an enterprise? Why? (10 Pts.)

4) Why would you recommend managing UNIX servers with ssh instead of telnet? Can this create more security issues? (5 Pts.)

5) Explain the following:

   Risk:

   Threat:

   Non-repudiation:

   False positive: (10 Pts.)

6) What are the IT security threats when a company laptop is stolen? How could you prevent them? Does it make a difference whether the laptop is on stand-by or powered off at the time of theft? Please explain. (10 Pts.)

7) What could be the impact, if an attacker finds a way to poison the cache of your main proxy server? Can he/she use this to hijack online banking transactions? Please support your arguments. (10 Pts.)
8) Adobe releases security updates to its products periodically. Company Y decides to replace Adobe Acrobat Reader and use an other PDF reader with the argument that Y doesn’t have the technology to implement the patches on a timely fashion. How would you rate this decision? Please explain. (10 Pts.)

9) Company Z has its web application and database servers placed in a DMZ, protected by a network firewall. Each packet sent/received from Internet to/from DMZ is filtered by the firewall according the following ruleset:

<table>
<thead>
<tr>
<th>Order</th>
<th>Protocol</th>
<th>Source Host</th>
<th>Source Port/</th>
<th>Destination Host</th>
<th>Destination Port</th>
<th>Permit/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>WebServer1</td>
<td>Https</td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td>ICMP</td>
<td>Any</td>
<td>*</td>
<td>WebServer1</td>
<td>*</td>
<td>Permit</td>
</tr>
<tr>
<td>3</td>
<td>UDP</td>
<td>SQLServer1</td>
<td>Any</td>
<td>DNSresolver1</td>
<td>DNS</td>
<td>Permit</td>
</tr>
<tr>
<td>4</td>
<td>ICMP</td>
<td>WebServer1</td>
<td>*</td>
<td>Any</td>
<td>*</td>
<td>Permit</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

* means any icmp message

Rules are processed from top to bottom. When a match occurs rest of the rules are discarded.

Webserver is hosting a single web page, which only receives input and does not give back any output to the client. The page processes critical data and stores it in the database.

During a security check, an easy to spot sql injection flaw is discovered. The flaw lets an attacker upload and execute code on the back-end database. Detailed analysis shows, that an attacker took over the control of db, but not the front-end server.

a. Based on the information above, is it possible to say, that the sensitive data could be stolen? Why/why not? Please explain in details. (25 Pts.)

b. Is the impact regarding data theft same/different, if the attacker discovered a remote code execution flaw affecting the web server software instead of the sql injection? What would you recommend to this company against such a flaw? (10 Pts.)

10) An attacker sends 1000 http requests per second to your front-end web server for more than a day. Which part of CIA covers this? (10 Pts.)

Good Luck!

Ertunga Arsal