Handout

Nakula & Antareja Incident

Lars Molske, Damian Nowak

5.5th Bieleschweig Workshop
Bielefeld, June 6-7 2005
Loss of resources

1.1 Attacker used Nakula unauthorized

1.1.1 Attacker used gained login/password combination for Nakula machine

1.1.2 Assumption: Attackers motivation: infiltrate hosts

1.1.1.1 Attacker sniffed network traffic

1.1.1.1.1 Switch operates in broadcast mode

1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded

1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic

1.1.1.1.2.1 Attacker accessed University Intranet

1.1.1.1.2.1.1 Attacker able to access University Intranet

1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

1.1.1.1.2.1.2 Need for FTP service in the RVS

1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment

1.1.1.2 Attacker gained valid login/password combination for Nakula machine

1.1.1.2.1 Unencrypted FTP connections used

1.1.1.2.1.1 Unencrypted FTP service offered on Nakula

1.1.1.2.1.1.1 ProFTPD installed and running on Nakula

1.1.1.3 RVS decision: Policy: Only trusted users are authorized to access Nakula

1.1.1.3.1 RVS decision: FTP login equals SSH login on Nakula
1.1 Attacker used Nakula unauthorized

1.2 Attacker used Antareja unauthorized

1.2.1 Attacker used gained login/password combination for Antareja machine

1.2.2 RVS Staff decision: Policy: Only trusted users are authorized to access Antareja

1.2.1.1 Attacker gained valid login/password combination for Antareja machine

1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text

1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja

1.2.1.1.2 Unencrypted FTP connections used

1.2.1.2 Attacker sniffed network traffic using Nakula

1.2.1.2.1 Attacker installed and launched sniffer undetected

1.2.1.2.1.1 Attacker installed rootkit on Nakula

1.2.1.2.1.1.1 Attacker gained root access on Nakula

1.2.1.2.1.1.1.1 Assumption: Attackers motivation: Collect further data from network traffic

1.2.1.2.2 Assumption: Attackers motivation: Gain root access on host

1.2.1.2.1.2 Local exploit on Nakula

1.2.1.1.1.1 RVS decision: Use ProFTP to fulfill need

1.2.1.1.1.1.1 ProFTP installed and running on Antareja

1.2.1.1.2 Need for FTP service in RVS

1.2.1.1.2.1 Assumption: Attackers motivation: Hide operations, avoid detection

1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic

1.2.1.1.2.3 HRZ guaranteed protection against sniffer attacks in a switched network environment

1.2.1.1.2.4 HRZ guaranteed protection against sniffer attacks in a switched network environment
## Factors meeting the presented criteria

<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
<th>Qualified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1.1.3:</td>
<td>RVS decision: FTP Login equals SSH Login on Antareja</td>
<td>L</td>
</tr>
<tr>
<td>1.2.1.2.1.1.1.2:</td>
<td>Local exploit on Nakula</td>
<td>L</td>
</tr>
<tr>
<td>1.1.1.1:</td>
<td>Attacker gained valid login/password comb. for Nakula mach.</td>
<td>SP</td>
</tr>
<tr>
<td>1.2.1.1:</td>
<td>Attacker gained valid login/password comb. for Antareja mach.</td>
<td>SP</td>
</tr>
<tr>
<td>1.1.1.1.3:</td>
<td>RVS decision: FTP Login equals SSH Login on Nakula</td>
<td>L</td>
</tr>
<tr>
<td>1.1.1.2.1:</td>
<td>Unencrypted FTP connections used on Nakula</td>
<td>4IO</td>
</tr>
<tr>
<td>1.2.1.1.1.1:</td>
<td>Unencrypted FTP connections used on Antareja</td>
<td>4IO</td>
</tr>
<tr>
<td>1.1.1.1.1.1.1:</td>
<td>Switch is configured to switch to broadcast mode when flooded</td>
<td>L</td>
</tr>
<tr>
<td>1.1.1.2.1.1.1.1:</td>
<td>RVS decision: Use ProFTP to fulfill need</td>
<td>4IO</td>
</tr>
<tr>
<td>1.1.1.1.1.2:</td>
<td>Insufficient network security provided by HRZ</td>
<td>L</td>
</tr>
</tbody>
</table>

The following facts meet the criteria, but we can intuitively judge that their direct elimination would not solve the problem:

<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
<th>Qualified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.1.1:</td>
<td>Examination of Antareja</td>
<td>5IO</td>
</tr>
<tr>
<td>1.4.2:</td>
<td>Examination of Nakula</td>
<td>6IO</td>
</tr>
<tr>
<td>1.3.1.1.2:</td>
<td>Detection by RVS: Unauthorized use of Antareja</td>
<td>L</td>
</tr>
<tr>
<td>1.4.2.1:</td>
<td>Detection by RVS: Unauthorized use of Antareja</td>
<td>L</td>
</tr>
<tr>
<td>1.3.1.1:</td>
<td>RVS decision: Policy: All incidents must be examined</td>
<td>L</td>
</tr>
<tr>
<td>1.1.3:</td>
<td>Only trusted users are authorized to use RVS hosts</td>
<td>L</td>
</tr>
<tr>
<td>1.1.1.2.1.2:</td>
<td>Need for FTP service in the RVS</td>
<td>5IO, L</td>
</tr>
</tbody>
</table>

---

1 \(x\) = Quantity of in- and out- edges, with \(x\) specifying the amount  
L = Leaves  
SP = Single point of failure