Yet Another tool to analyze BruteSSH attacks

UNAM-CERT
Problem

• Common account names (www, guest, adm)
• Weak passwords
• Speed is no longer an issue
• Lots of ssh probes per day, hour, minute...
• Need to report and block these events
The tool

• It is one of the most useful tools for the university
• Actually in development
• All the tools used are shell based
  – Awk
  – Sed
  – Cat, find, etc.
BruteSSH attacks detection tool

- Read ssh-log files looking for failed login attempts
- Unix shell based
- Gather IP information
  - victim
  - date
  - start time
  - source IP
  - responsible (whois)
  - Country
BruteSSH attacks detection tool

- Alert system (e-mail)
- Diary Summary
- Report by IP
- HTML Report
- GNU Plot graphs
- Victim summary in html (how many attacks does it receive?)
### Attack Summary

---

**Brute-SSH attacks summary 09262005**

---

**System affected:** honeybot

3513 attacks received

---

- 1437 to root account
- 2076 to unprivileged accounts

---

**Source IP’s (University)**

---

1 132.248.132.4

---

**Source IP’s (external)**

---

<table>
<thead>
<tr>
<th>Number</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>64.139.133.174</td>
</tr>
<tr>
<td>37</td>
<td>209.67.215.146</td>
</tr>
<tr>
<td>24</td>
<td>211.75.113.237</td>
</tr>
<tr>
<td>19</td>
<td>211.21.210.229</td>
</tr>
<tr>
<td>18</td>
<td>220.70.167.67</td>
</tr>
<tr>
<td>15</td>
<td>69.57.148.99</td>
</tr>
<tr>
<td>13</td>
<td>211.219.30.145</td>
</tr>
</tbody>
</table>
Further work

- Real-Time monitoring (research proposes)
- Active Response (iptables, ipf, pf, tcp-wrappers)
- Analyze additional attacks
- Windows Version