## Appendix A: Attacks in Test Data Set 1

<table>
<thead>
<tr>
<th>Week</th>
<th>Day</th>
<th>Attack Name</th>
<th>Time</th>
<th>Source Machine</th>
<th>Dest Machine</th>
<th>User</th>
<th>Where</th>
<th>Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Mon</td>
<td>pf</td>
<td>13:02:04</td>
<td>135.8.60.182</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Mon</td>
<td>satan</td>
<td>17:29:28</td>
<td>202.72.1.77</td>
<td>Zeno</td>
<td>-</td>
<td>tcp</td>
<td>level 0</td>
</tr>
<tr>
<td>6</td>
<td>Mon</td>
<td>neptune</td>
<td>19:19:17</td>
<td>9.9.9.9</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td>port 20,23,79,80</td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>portsweep</td>
<td>08:16:51</td>
<td>206.48.44.18</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td>ACK, every 38 secs, ports 1-2000</td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>pod</td>
<td>13:04:56</td>
<td>207.103.80.104</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>10 oversize ping packets</td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>land</td>
<td>17:53:49</td>
<td>Zeno</td>
<td>Zeno</td>
<td>-</td>
<td>tcp</td>
<td>port 23</td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>ipsweep</td>
<td>08:29:08</td>
<td>209.30.70.14</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>nmap -u -n -p53 (udp scan for named)</td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>neptune</td>
<td>10:41:42</td>
<td>135.13.216.191</td>
<td>Zeno</td>
<td>-</td>
<td>tcp</td>
<td>all ports for an hour</td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>back</td>
<td>14:11:52</td>
<td>135.8.60.182</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>ipsweep</td>
<td>08:27:03</td>
<td>205.231.28.163</td>
<td>172.16.11.4</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>ipsweep</td>
<td>08:28:43</td>
<td>196.37.75.158</td>
<td>172.16.11.2</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>eject</td>
<td>08:41:50</td>
<td>202.247.224.89</td>
<td>pascal</td>
<td>raeburnt</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>fb</td>
<td>09:06:46</td>
<td>196.174.194.16</td>
<td>pascal</td>
<td>alie</td>
<td>tcp,bm</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>eject</td>
<td>09:32:03</td>
<td>135.8.60.182</td>
<td>pascal</td>
<td>alie</td>
<td>tcp,bm</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>eject</td>
<td>09:50:46</td>
<td>195.73.151.50</td>
<td>pascal</td>
<td>alie</td>
<td>tcp,bm</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>eject</td>
<td>10:00:14</td>
<td>135.8.60.182</td>
<td>pascal</td>
<td>alie</td>
<td>tcp,bm</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>pod</td>
<td>10:11:06</td>
<td>135.13.216.191</td>
<td>pc0</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>pod</td>
<td>10:20:11</td>
<td>209.30.71.165</td>
<td>linux10</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>pod</td>
<td>10:27:24</td>
<td>207.103.80.104</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>dict</td>
<td>10:34:46</td>
<td>206.186.80.111</td>
<td>Marx</td>
<td>kiarra</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>ipsweep</td>
<td>10:37:42</td>
<td>202.72.1.77</td>
<td>172.16.11.2</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>pf</td>
<td>11:15:53</td>
<td>209.74.60.168</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>neptune</td>
<td>11:32:23</td>
<td>230.1.10.20</td>
<td>Pascal</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>portsweep</td>
<td>12:03:45</td>
<td>202.247.224.89</td>
<td>Zeno</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>eject</td>
<td>12:21:55</td>
<td>209.12.13.144</td>
<td>Pascal</td>
<td>raeburnt</td>
<td>tcp,bm</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>portsweep</td>
<td>12:29:51</td>
<td>207.103.80.104</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>smurf</td>
<td>12:48:13</td>
<td>*</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>land</td>
<td>13:31:05</td>
<td>*</td>
<td>*</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>neptune</td>
<td>13:31:08</td>
<td>10.20.30.40</td>
<td>Pascal</td>
<td>-</td>
<td>tcp</td>
<td>-</td>
</tr>
<tr>
<td>Week</td>
<td>Day</td>
<td>Attack Name</td>
<td>Time</td>
<td>Source Machine</td>
<td>Dest Machine</td>
<td>User</td>
<td>Where</td>
<td>Variant</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>-------------</td>
<td>----------</td>
<td>----------------</td>
<td>--------------</td>
<td>------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>satan</td>
<td>08:04:25</td>
<td>207.230.54.203</td>
<td>marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>syslog</td>
<td>12:42:51</td>
<td>1.1.1.1</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>phf</td>
<td>15:53:54</td>
<td>197.182.91.233</td>
<td>marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>land</td>
<td>18:48:49</td>
<td>Several</td>
<td>several</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>portsweep</td>
<td>13:05:46</td>
<td>194.27.251.21</td>
<td>marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>pod</td>
<td>16:34:52</td>
<td>207.103.80.104</td>
<td>marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>ffb</td>
<td>17:10:01</td>
<td>206.47.98.151</td>
<td>pascal alie</td>
<td>tcp</td>
<td>No bsm</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>eject</td>
<td>19:16:45</td>
<td>209.74.60.168</td>
<td>pascal raeburnt</td>
<td>tcp</td>
<td>No bsm</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>phf</td>
<td>08:56:59</td>
<td>205.180.112.36</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>loadmodule</td>
<td>09:41:51</td>
<td>209.12.13.144</td>
<td>Zeno simple1</td>
<td>tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>teardrop</td>
<td>12:53:40</td>
<td>222.222.222.222</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>ipsweep</td>
<td>18:01:10</td>
<td>207.114.237.57</td>
<td>172.16.11</td>
<td>tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>portsweep</td>
<td>23:10:42</td>
<td>128.223.199.68</td>
<td>Zeno</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>smurf</td>
<td>17:46:58</td>
<td>*</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>satan</td>
<td>21:40:40</td>
<td>207.75.239.115</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>perlmagic</td>
<td>22:09:33</td>
<td>135.8.60.182</td>
<td>Marx alie</td>
<td>tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>ipsweep</td>
<td>23:53:54</td>
<td>153.37.134.17</td>
<td>172.16.11</td>
<td>tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fri</td>
<td>neptune</td>
<td>09:48:11</td>
<td>10.20.30.40</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fri</td>
<td>smurf</td>
<td>17:16:23</td>
<td>10.different</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fri</td>
<td>neptune</td>
<td>19:21:20</td>
<td>9.9.9.9</td>
<td>pascal</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fri</td>
<td>back</td>
<td>22:51:38</td>
<td>207.75.239.115</td>
<td>Marx</td>
<td>-</td>
<td>tcp</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C: Attacks in Test Data Set 3

ID: 41.084031 Date: 03/29/1999 Name: ps Category: u2r
Start Time: 08:18:35 Duration: 00:46:05 Attacker: 209.154.098.104
Victim: 172.016.112.050 Username: harald
Ports: At_Attacker: 80(1), 6000(2) At_Victim: 23(3)

ID: 41.084818 Date: 03/29/1999 Name: sendmail Category: r2l
Start Time: 08:48:12 Duration: 00:00:02 Attacker: 202.049.244.010
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 113(1) At_Victim: 25(1)

ID: 41.090000 Date: 03/29/1999 Name: New_Attack_1999 (ntfsdos)
Category: r2l Start Time: 09:08:00 Duration: 00:08:00 Attacker: 172.16.112.100
Victim: 172.16.112.100 Username: n/a
Ports: At_Attacker: At_Victim: i(2)

ID: 41.091531 Date: 03/29/1999 Name: portsweep Category: probe
Start Time: 09:15:05 Duration: 00:20:32 Attacker: 172.016.118.020
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: At_Victim: 25(1), 80(1), 143(1)

ID: 41.093708 Date: 03/29/1999 Name: New_Attack_1999 (sshtrojanInstall)
Category: r2l Start Time: 09:36:23 Duration: 00:05:13
Attacker: 202.077.162.213 Victim: 172.016.114.050
Username: virginii anonymous failed: host
Ports: At_Attacker: 20(3), 113(1) At_Victim: 23(1), 25(1)

ID: 41.111531 Date: 03/29/1999 Name: portsweep Category: probe
Start Time: 11:15:15 Duration: 00:04:01 Attacker: 172.016.118.050
Victim: 192.168.001.001 Username: n/a
Ports: At_Attacker: At_Victim: 21-22(1), 25(1), 80(1), 513(1)

ID: 41.112127 Date: 03/29/1999 Name: xsnoop Category: r2l
Start Time: 11:22:43 Duration: 00:01:17 Attacker: 128.223.199.068
Victim: 172.016.114.168 Username: n/a
Ports: At_Attacker: At_Victim: 6000(1)

ID: 41.114554 Date: 03/29/1999 Name: snmpget Category: r2l
Start Time: 11:45:12 Duration: 00:33:31 Attacker: 204.097.153.043
Victim: 172.016.000.001 Username: n/a
Ports: At_Attacker: At_Victim: 161/u(501)

ID: 41.114703 Date: 03/29/1999 Name: guesstelnet Category: r2l
Start Time: 11:47:16 Duration: 00:00:10 Attacker: 192.005.041.239
Victim: 172.016.113.050 Username: emonic
Ports: At_Attacker: At_Victim: 23(7)

ID: 41.122222 Date: 03/29/1999 Name: portsweep Category: probe
Start Time: 12:22:15 Duration: 00:05:01 Attacker: 153.107.252.061
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 21-22(1), 25(1), 80(1)
ID: 41.133333 Date: 03/29/1999 Name: guessftp Category: r21
Start_Time: 13:33:16 Duration: 00:00:22 Attacker: 172.016.118.070
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: 1050-1052(1), 1054(1), 1104(1) At_Victim: 21(5)

Ports: At_Attacker: At_Victim: 20-21(1), 513(1)

Ports: At_Attacker: At_Victim: 23(2), 80(1)

ID: 41.161308 Date: 03/29/1999 Name: crashiiis Category: dos
Start_Time: 16:13:08 Duration: 00:00:05 Attacker: 172.016.118.070
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 80(1)

ID: 41.162715 Date: 03/29/1999 Name: portsweep Category: probe
Start_Time: 16:27:10 Duration: 00:04:56 Attacker: 202.077.162.213
Victim: 172.016.114.169 Username: n/a
Ports: At_Attacker: At_Victim: 21(2), 23(2), 25(2), 79(2), 143(2)

ID: 41.182453 Date: 03/29/1999 Name: New Attack 1999 (secret)
Category: data Start_Time: 19:24:19 Duration: 00:08:41
Ports: At_Attacker: 25(1) At_Victim: 23(1), 113(1)

ID: 41.213446 Date: 03/29/1999 Name: smurf Category: dos
Start_Time: 21:34:16 Duration: 00:00:11 Attacker: 006.238.105.108
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: i(398)

ID: 42.090909 Date: 03/30/1999 Name: httptunnel Category: r21
Start_Time: 09:09:17 Duration: 00:02:39 Attacker: 197.182.091.233
Victim: 172.016.112.050 Username: rexn o format login /var/adm/lastlog
Ports: At_Attacker: 20-21(1) At_Victim: 23(1)

ID: 42.094131 Date: 03/30/1999 Name: phf Category: r21
Start_Time: 09:41:12 Duration: 00:00:01 Attacker: 202.247.224.089
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 80(1)

ID: 42.104107 Date: 03/30/1999 Name: loadmodule Category: u2r
Start_Time: 10:10:12 Duration: 00:26:10 Attacker: 194.027.251.021
Victim: 172.016.113.050 Username: marlyy
Ports: At_Attacker: At_Victim: 23(1)

ID: 42.112913 Date: 03/30/1999 Name: ps Category: u2r
Start_Time: 11:29:17 Duration: 00:35:52 Attacker: 206.222.003.197
Victim: 172.016.112.050 Username: bramy
Ports: At_Attacker: At_Victim: 20-21(1), 23(1)

ID: 42.120000 Date: 03/30/1999 Name: New Attack 1999 (ntfstdos)
Category: r21 Start_Time: 12:00:00 Duration: 00:10:00
Attacker: 172.16.112.100 Victim: 172.16.112.100 Username: n/a
ID: 42.122248 Date: 03/30/1999 Name: New Attack 1993 (secret)
Category: data Start Time: 12:22:13 Duration: 00:52:29
Attacker: 197.218.177.069 Victim: 172.016.114.050 Username: quintonsp
TTY Ports: At_Attacker: 20-21(1), 25(1), 113(1) At_Victim: 23(1), 25(1), 113(1)

ID: 42.135452 Date: 03/30/1999 Name: sqlattack Category: r21
Start Time: 13:54:17 Duration: 00:01:09 Attacker: 207.253.084.013
Victim: 172.016.112.194 Username: db3 Ports: At_Attacker: At_Victim: 23(1)

ID: 42.143228 Date: 03/30/1999 Name: New Attack 1993 (sechole)
Category: u2r Start Time: 14:32:15 Duration: 05:04:52 Attacker: 205.160.208.190
Victim: 172.016.112.100 Username: n/a Ports: At_Attacker: At_Victim: 20(2), 21(1), 23(2)

ID: 42.145441 Date: 03/30/1999 Name: land Category: dos Start Time: 14:54:10 Duration: 00:00:01
Attacker: 172.016.113.050 Victim: 172.016.113.050 Username: n/a Ports: At_Attacker: At_Victim: 23(1)

ID: 42.155148 Date: 03/30/1999 Name: mailbomb Category: dos
Start Time: 15:51:16 Duration: 00:11:24 Attacker: 194.027.251.021
Victim: 172.016.114.050 Username: n/a Ports: At_Attacker: i(1), 25(3), 110(1), 113(200)
At_Victim: 25(200)

ID: 42.174944 Date: 03/30/1999 Name: processtable Category: dos
Start Time: 17:49:15 Duration: 00:03:01 Attacker: 209.240.124.083
Victim: 172.016.114.050 Username: n/a Ports: At_Attacker: At_Victim: 22(352)

ID: 42.210410 Date: 03/30/1999 Name: crashkills Category: dos
Start Time: 21:04:10 Duration: 00:00:07 Attacker: 209.001.012.046
Victim: 172.016.112.100 Username: n/a Ports: At_Attacker: At_Victim: 80(1)

ID: 43.080401 Date: 03/31/1999 Name: satan Category: probe
Start Time: 08:04:14 Duration: 00:00:13 Attacker: 209.030.070.014
Victim: 172.016.114.050 Username: n/a Ports: At_Attacker: i(2), 113(1)
At_Victim: i(1), 21(1), 23(2), 25(1), 70(1), 79(6), 80(1), 111(1), 119(1), 540(1), 6000(1), 177/u(1)

ID: 43.084000 Date: 03/31/1999 Name: New Attack 1999 (netcat)
Category: r21 Start Time: 09:26:12 Duration: 00:00:04
Attacker: 207.230.054.203 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25(1)

ID: 43.093814 Date: 03/31/1999 Name: imap Category: r21
Start Time: 09:38:13 Duration: 00:00:53 Attacker: 208.254.251.132
Victim: 172.016.114.050 Username: n/a Ports: At_Attacker: At_Victim: 143(1)

ID: 43.100000 Date: 03/31/1999 Name: New Attack 1999 (ppmarcro)
Category: r21 Start Time: 10:14:36 Duration: 00:13:01
Attacker: 194.027.251.021 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25(1), 80(6)

D: 43.10313 Date: 03/31/1999 Name: procsstable Category: dos
Start_Time: 10:13:18 Duration: 00:28:02 Attacker: 172.016.118.060
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker:   At_Victim: 25(367)

D: 43.103931 Date: 03/31/1999 Name: fdformat Category: u2r
Start_Time: 10:38:00 Duration: 00:03:00 Attacker: console
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker:   At_Victim:   

ID: 43.110000 Date: 03/31/1999 Name: New Attack 1999 (netcat)
Category: r21 Start_Time: 11:11:08 Duration: 00:00:32
Attacker: 206.048.044.018 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker:   At_Victim: 53(1)

ID: 43.111111 Date: 03/31/1999 Name: New Attack 1999 (warezmaster)
Category: dos Start_Time: 11:25:39 Duration: 00:00:47
Attacker: 202.027.121.118 Victim: 172.016.112.050
Username: anonymous Ports: At_Attacker:   At_Victim: 20-21(1)

ID: 43.113032 Date: 03/31/1999 Name: New Attack 1999 (arppoison)
Category: probe Start_Time: 11:30:13 Duration: 00:11:21
Ports: At_Attacker:   At_Victim:   

ID: 43.114500 Date: 03/31/1999 Name: ncftp Category: r21
Start_Time: 12:12:38 Duration: 00:01:29 Attacker: 152.169.215.104
Victim: 172.016.114.050 Username: bramy anonymous
Ports: At_Attacker: 20(6), 21(1), 25(1)   At_Victim: 23(1), 113(1)

ID: 43.122854 Date: 03/31/1999 Name: New Attack 1999 (secret)
Category: data Start_Time: 12:28:15 Duration: 00:08:12
Attacker: 196.037.075.158 Victim: 172.016.112.050 Username: elmoc tty
Ports: At_Attacker: 20-21(1) At_Victim: 23(1)

ID: 43.125900 Date: 03/31/1999 Name: named Category: r21
Start_Time: 13:00:32 Duration: 00:05:10 Attacker: 194.007.248.153
Victim: 172.016.112.020 Username: katjab
Ports: At_Attacker: 6000(1) At_Victim: 53(1)

ID: 43.134223 Date: 03/31/1999 Name: guessftp Category: r21
Start_Time: 13:42:16 Duration: 00:01:56 Attacker: 208.240.124.083
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker:   At_Victim: 21(75)

ID: 43.144547 Date: 03/31/1999 Name: smurf Category: dos
Start_Time: 18:29:25 Duration: 00:00:01 Attacker: 001.012.120.006
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker:   At_Victim: i(253)

ID: 43.155357 Date: 03/31/1999 Name: guest
Category: r21 Start_Time: 15:53:15 Duration: 00:02:43
3118 3072 Ports:   At_Attacker:   At_Victim: 23(9)
ID: 43.164334 Date: 03/31/1999 Name: portsweep Category: probe
Start Time: 16:43:15 Duration: 00:03:54 Attacker: 208.240.124.083
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 19(1), 79(1), 143(1)

ID: 43.165422 Date: 03/31/1999 Name: mailbomb Category: dos
Start Time: 16:54:17 Duration: 00:03:01 Attacker: 194.007.248.153
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 25(150)

ID: 43.175811 Date: 03/31/1999 Name: guesstelnet Category: r21
Start Time: 17:58:17 Duration: 00:03:48 Attacker: 209.001.012.046
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 23(20)

ID: 43.191217 Date: 03/31/1999 Name: snmpget Category: r21
Start Time: 19:12:16 Duration: 00:16:57
Attacker: 207.191.092.211 Victim: 172.016.000.001
Username: n/a Ports: At_Attacker: At_Victim: 161/1(u(201)

ID: 44.080000 Date: 04/01/1999 Name: ntinfoscan Category: probe
Start Time: 08:00:03 Duration: 00:16:01 Attacker: 172.016.112.103
Victim: 206.043.044.018 Username: n/a
Ports: At_Attacker: 204(1), 23(1), 80(11), 139(2) At_Victim: 1041(1)

ID: 44.080757 Date: 04/01/1999 Name: ipsweep Category: probe
Start Time: 08:07:11 Duration: 00:01:32 Attacker: 172.016.112.015, 194.027.251.021 Victim: 172.016.112.010, 194.027.251.021 Username: n/a
Ports: At_Attacker: i(2) At_Victim: i(10)

ID: 44.082615 Date: 04/01/1999 Name: teardrop Category: dos Start Time: 08:26:20 Duration: 00:00:01 Attacker: 172.016.118.060
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 80/u(1)

ID: 44.083000 Date: 04/01/1999 Name: New_Attack_1999 (netbus)
Category: r21 Start Time: 08:35:11 Duration: 00:06:04
Attacker: 135.008.060.182 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25(1), 12345-12346(1)

ID: 44.091807 Date: 04/01/1999 Name: New_Attack_1999 (sshtrojan)
Category: r21 Start Time: 09:38:15 Duration: 00:10:30
Attacker: 195.073.151.050 Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 22(2)

ID: 44.110000 Date: 04/01/1999 Name: New_Attack_1999 (doscnuke)
Category: dos Start Time: 11:00:07 Duration: 00:01:33
Attacker: 172.016.115.234 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 139(1)

ID: 44.114500 Date: 04/01/1999 Name: ncftp Category: r21
Start Time: 11:45:14 Duration: 00:01:28 Attacker: 172.016.118.043
Victim: 172.016.114.050 Username: bramy anonymous
Ports: At_Attacker: 20(7), 21(1) At_Victim: 23(1)

ID: 44.120500 Date: 04/01/1999 Name: New_Attack_1999 (ppmarcro)
ID: 44.124700 Date: 04/01/1999 Name: guest Category: r21
Start Time: 12:56:47 Duration: 00:02:42 Attacker: 153.107.252.061
Victim: 172.016.112.050 Username: guest 2270 2189 872
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25(1), 80(5)

ID: 44.130700 Date: 04/01/1999 Name: xlock Category: r21
Start Time: 13:08:19 Duration: 00:00:25 Attacker: 209.012.013.144
Victim: 172.016.112.168 Username: n/a
Ports: At_Attacker: At_Victim: 6000[2]

ID: 44.131529 Date: 04/01/1999 Name: guesspop Category: r21
Start Time: 13:15:16 Duration: 00:02:11 Attacker: 202.247.224.089
Victim: 172.016.112.194 Username: Bad
Ports: At_Attacker: At_Victim: 110(30)

ID: 44.161242 Date: 04/01/1999 Name: phf Category: r21
Start Time: 16:12:15 Duration: 00:00:01 Attacker: 202.072.001.077
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 80(1)

ID: 44.164944 Date: 04/01/1999 Name: New_Attack_1999 (sshprocesstable)
Category: dos Start Time: 16:49:15 Duration: 00:08:21
Attacker: 172.016.118.020 Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 22(490)

ID: 44.183234 Date: 04/01/1999 Name: mailbomb Category: dos
Start Time: 18:32:17 Duration: 00:10:07 Attacker: 194.027.251.021
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 25(500)

ID: 44.201454 Date: 04/01/1999 Name: sqlattack Category: r21
Start Time: 20:14:17 Duration: 00:01:08 Attacker: 194.007.248.153
Victim: 172.016.112.194 Username: db3
Ports: At_Attacker: At_Victim: 23(1)

ID: 45.084547 Date: 04/02/1999 Name: smurf Category: dos
Start Time: 08:45:18 Duration: 00:00:02 Attacker: 001.012.120.006
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: i(253)

ID: 45.090000 Date: 04/02/1999 Name: New_Attack_1999 (arppoison)
Category: probe Start Time: 09:00:10 Duration: 00:12:51
Ports: At_Attacker: At_Victim:

ID: 45.095541 Date: 04/02/1999 Name: New_Attack_1999 (sshtrojan)
Category: r21 Start Time: 09:55:15 Duration: 00:10:29
Attacker: 195.073.151.050 Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 22(2)

ID: 45.100334 Date: 04/02/1999 Name: ipsweep
Category: probe Start Time: 10:03:10 Duration: 00:15:01
Attacker: 172.016.112.005, 172.016.112.010, 194.007.248.153
Victim: 172.016.112.001-010, 194.007.248.153 Username: n/a
Ports: At_Attacker: i(2) At_Victim: i(10)
ID: 45.103937 Date: 04/02/1999 Name: xlock Category: r21
Start Time: 10:42:04 Duration: 00:01:19 Attacker: 139.134.061.042
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 6000[4]

ID: 45.105138 Date: 04/02/1999 Name: named Category: r21
Start Time: 10:53:24 Duration: 00:03:35 Attacker: 194.007.248.153
Victim: 172.016.112.020 Username: n/a

ID: 45.111010 Date: 04/02/1999 Name: portsweep Category: probe
Start Time: 11:10:15 Duration: 00:04:31 Attacker: 208.240.124.083
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: i(2) At_Victim: i(2), 17/u(1), 19/u(2), 23/u(1), 37/u(2), 514/u(2)

ID: 45.114500 Date: 04/02/1999 Name: ncftp Category: r21
Start Time: 11:45:13 Duration: 00:01:29 Attacker: 172.016.118.070
Victim: 172.016.113.050 Username: anonymous

ID: 45.114900 Date: 04/02/1999 Name: New Attack 1999 (netbus) Category: r21
Start Time: 11:51:00 Duration: 00:04:13
Attacker: 209.001.012.046 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25[1], 12345-12346[1]

ID: 45.123234 Date: 04/02/1999 Name: mailbomb Category: dos
Start Time: 12:32:17 Duration: 00:12:59 Attacker: 202.072.001.077
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: 4338[1] At_Victim: 25[500]

ID: 45.130542 Date: 04/02/1999 Name: named Category: r21
Start Time: 13:49:30 Duration: 00:00:58 Attacker: 195.073.151.050
Victim: 172.016.112.020 Username: n/a

ID: 45.140000 Date: 04/02/1999 Name: ipsweep Category: probe
Ports: At_Attacker: At_Victim: i(5)

ID: 45.162148 Date: 04/02/1999 Name: loadmodule Category: u2r
Start Time: 16:21:16 Duration: 00:05:41 Attacker: 194.027.251.021
Victim: 172.016.113.050 Username: warcd
Ports: At_Attacker: At_Victim: 23[1]

ID: 45.165009 Date: 04/02/1999 Name: New Attack 1999 (sechole) Category: u2r
Start Time: 16:50:15 Duration: 00:45:11
Attacker: 195.115.218.108 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 20[2], 21[1], 23[2]

ID: 45.181011 Date: 04/02/1999 Name: portsweep Category: probe
Start Time: 18:10:15 Duration: 00:00:05 Attacker: 202.049.244.010
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: 7(1), 19(1), 21-22(1), 25(1)

ID: 45.192523 Date: 04/02/1999 Name: ipsweep
Category: probe Start Time: 19:25:14 Duration: 00:42:18
Attacker: 172.016.112.005, 172.016.112.010, 172.016.112.050,
172.016.112.100, 172.016.112.194, 172.016.112.207, 172.016.113.105,
172.016.114.207, 194.007.248.153 Victim: 172.016.112.001-254,
194.007.248.153 Username: n/a
Ports: At_Attacker: i(8) At_Victim: i(254)

ID: 45.203400 Date: 04/02/1999 Name: New Attack 1999 (secret)
Category: data Start Time: 20:34:00 Duration: 00:02:00
Attacker: console Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim:
Appendix D: Attacks in Test Data Set 4

ID: 51.0833800 Date: 04/05/1999 Name: pod Category: dos
Start_Time: 08:39:52 Duration: 00:00:10 Attacker: 202.077.162.213
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: i{1}

ID: 51.084334 Date: 04/05/1999 Name: portswipe Category: probe
Start_Time: 08:43:17 Duration: 00:03:53 Attacker: 172.016.118.010
Victim: 192.168.001.001 Username: n/a
Ports: At_Attacker: At_Victim: 79-80{1}, 143{1}

ID: 51.085000 Date: 04/05/1999 Name: pod Category: dos
Start_Time: 08:48:33 Duration: 00:00:31 Attacker: 202.077.162.213
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: i{1}

ID: 51.085947 Date: 04/05/1999 Name: New_Attack 1999 (warezclient)
Category: dos Start_Time: 08:59:16 Duration: 00:00:41
Attacker: 207.075.239.11b Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 20-21{1}

ID: 51.093123 Date: 04/05/1999 Name: smurf Category: dos
Start_Time: 09:33:00 Duration: 00:02:00 Attacker: login.session.x.x
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: i{1531}

ID: 51.094334 Date: 04/05/1999 Name: portswipe Category: probe
Start_Time: 09:43:11 Duration: 00:03:43 Attacker: 208.240.124.083
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 1-6{1}, 7{2}, 8{1}, 9{2}, 10-12{1},
13{2}, 14-18{1}, 19{2}, 20{1}, 21-23{2}, 24{1}, 25{2}, 26-36{1}, 37{2},
38-52{1}, 54-78{1}, 79{2}, 80-100{1}

ID: 51.102700 Date: 04/05/1999 Name: apache2 Category: dos
Start_Time: 10:29:22 Duration: 00:17:37 Attacker: 202.077.162.213
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 1389{1} At_Victim: 80{1014}

ID: 51.105811 Date: 04/05/1999 Name: guesstelnet Category:r2l
Start_Time: 10:58:14 Duration: 00:03:20 Attacker: 192.005.041.239
Victim: 172.016.118.080 Username: n/a
Ports: At_Attacker: 37{1} At_Victim: 23{20}

ID: 51.1144500 Date: 04/05/1999 Name: New_Attack_1999 (dosnuke)
Category: dos Start_Time: 11:45:27 Duration: 00:01:33
Attacker: 172.016.115.234 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 139{1}

ID: 51.120309 Date: 04/05/1999 Name: loadmodule Category: u2r
Start_Time: 12:03:14 Duration: 00:11:15 Attacker: 172.016.114.207
Victim: 172.016.113.050 Username: elmoc
Ports: At_Attacker: At_Victim: 23{1}

143
ID: 51.121101 Date: 04/05/1999 Name: ffmpeg Category: u2r
Start_Time: 12:11:18 Duration: 00:12:28 Attacker: 135.013.216.191
Victim: 172.016.112.050 Username: henninmg
Ports: At_Attacker: At_Victim: 23{1}

ID: 51.131803 Date: 04/05/1999 Name: smurf Category: dos
Start_Time: 13:18:12 Duration: 00:00:01 Attacker: 023.234.078.052
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: i{429}

ID: 51.133019 Date: 04/05/1999 Name: New_Attack_1999 (arpdeco)
Category: probe Start_Time: 13:30:14 Duration: 00:14:37
Attacker: 152.169.215.104 Victim: 172.016.112.100 Username: abramh
Ports: At_Attacker: At_Victim:

ID: 51.140100 Date: 04/05/1999 Name: apache2 Category: dos
Start_Time: 14:05:43 Duration: 00:11:09 Attacker: 152.169.215.104
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 2275-2277(1), 2358(2), 2639(2), 2750(2), 2759(2),
2943(2), 3380(2), 3483(2), 3662(2), 3906(2)
At_Victim: 80(374)

ID: 51.142100 Date: 04/05/1999 Name: pod Category: dos
Start_Time: 14:22:30 Duration: 00:00:01 Attacker: 010.011.022.033
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: At_Victim: i(1)

ID: 51.144001 Date: 04/05/1999 Name: imap Category: r21
Start_Time: 14:46:19 Duration: 00:00:10 Attacker: 172.016.117.103
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 143{1}

ID: 51.150000 Date: 04/05/1999 Name: ipsweep Category: probe
Start_Time: 15:00:16 Duration: 05:15:21 Attacker: 128.223.199.068,
172.016.113.050, 204.071.051.016, 204.233.047.021, 207.114.237.057,
209.001.012.046
Victim: 172.016.113.001, 172.016.113.003-005, 172.016.113.050,
204.233.047.021
Username: n/a
Ports: At_Attacker: At_Victim: i(5)

ID: 51.163200 Date: 04/05/1999 Name: dict Category: r21
Start_Time: 16:32:17 Duration: 00:16:35 Attacker: 172.016.118.010
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 23{86}

ID: 51.171917 Date: 04/05/1999 Name: syslogd Category: dos
Start_Time: 17:19:10 Duration: 00:00:01 Attacker: 172.005.003.005
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 514/u(1)

ID: 51.180445 Date: 04/05/1999 Name: Neptune Category: dos
Start_Time: 18:04:04 Duration: 00:06:51 Attacker: 010.020.030.040
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 1-1024{20}
D: 51.183623 Date: 04/05/1999 Name: crashiis Category: dos
Start_Time: 18:36:11 Duration: 00:00:07 Attacker: 202.072.001.077
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 0 At_Victim: 80[1]

D: 51.185613 Date: 04/05/1999 Name: New_Attack 1999 (ls)
Category: probe Start_Time: 18:57:21 Duration: 00:00:01
Attacker: 195.073.151.050 Victim: 172.016.112.020 Username: n/a

D: 51.194715 Date: 04/05/1999 Name: New_Attack 1999 (donsuke)
Category: dos Start_Time: 19:48:01 Duration: 00:01:41
Attacker: 206.048.044.018 Victim: 172.016.115.234 Username: n/a
Ports: At_Attacker: At_Victim: 139[1]

D: 51.200037 Date: 04/05/1999 Name: udpstorm Category: dos
Start_Time: 20:00:27 Duration: 00:15:00 Attacker: 172.016.112.050
Victim: 172.016.112.113.* Username: n/a
Ports: At_Attacker: At_Victim: 7[1]

D: 51.201715 Date: 04/05/1999 Name: selfping Category: dos
Start_Time: 20:17:12 Duration: 00:00:03 Attacker: 135.013.216.191
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 23[1]

D: 51.204631 Date: 04/05/1999 Name: ncftp Category: r21
Start_Time: 20:46:13 Duration: 00:01:29 Attacker: 172.016.118.070
Victim: 172.016.114.050 Username: bramy anonymous
Ports: At_Attacker: 20[1], 21[1], 25[1] At_Victim: 23[1], 113[1]

D: 52.081109 Date: 04/06/1999 Name: New_Attack 1999 (tcpreset)
Category: probe Start_Time: 08:11:15 Duration: 00:10:50
Attacker: 135.008.060.182 Victim: 172.016.112.050 Username: lucyj
Ports: At_Attacker: At_Victim: 23[1]

D: 52.083236 Date: 04/06/1999 Name: teardrop Category: dos
Start_Time: 08:32:14 Duration: 00:00:01 Attacker: 207.230.054.203
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 23[1]

D: 52.085357 Date: 04/06/1999 Name: New_Attack 1999 (casesen)
Category: u2r Start_Time: 08:53:17 Duration: 00:49:38
Attacker: 172.016.113.204 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 20[3], 21[1], 23[2]

D: 52.092200 Date: 04/06/1999 Name: xsnnoop Category: r21
Start_Time: 09:19:01 Duration: 00:01:12 Attacker: 194.007.248.153
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 6000[1]

D: 52.094514 Date: 04/06/1999 Name: selfping Category: dos
Start_Time: 09:45:13 Duration: 00:00:03 Attacker: 192.182.091.233
Victim: 172.016.112.050 Username: bramy
Ports: At_Attacker: At_Victim: 23[1]

D: 52.100738 Date: 04/06/1999 Name: xterm1 Category: u2r
Start_Time: 10:07:18 Duration: 00:40:43 Attacker: 152.169.215.104
Victim: 172.016.112.194 Username: charlot
Ports: At Attacker: 20(2), 21(1), 23(1)

ID: 52.101901 Date: 04/06/1999 Name: ftpwrite Category: r21
Start Time: 10:19:16 Duration: 00:14:04
Attacker: 172.016.114.207 Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: 20(2), 21(1), 513(1)

ID: 52.103409 Date: 04/06/1999 Name: back Category: dos
Start Time: 11:31:21 Duration: 00:20:38 Attacker: 206.048.044.050
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 2222(1), 2234(1), 2234(1) At_Victim: 80(47)

ID: 52.112045 Date: 04/06/1999 Name: ps Category: u2r
Victim: 172.016.112.050 Username: bramy root `bram` `H` H
Ports: At_Attacker: 80(1), 6000(2) At_Victim: 23(2)

ID: 52.113855 Date: 04/06/1999 Name: Neptune Category: dos
Start Time: 11:38:04 Duration: 00:13:41 Attacker: 010.020.030.040
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 80(1), 1-1024(40)

ID: 52.120600 Date: 04/06/1999 Name: http_tunnel Category: r21
Start Time: 12:06:32 Duration: 00:03:30 Attacker: 172.016.112.050
Victim: 196.037.075.158 Username: n/a
Ports: At_Attacker: 8000(8)

ID: 52.125501 Date: 04/06/1999 Name: eject Category: u2r
Victim: 172.016.112.050 Username: harald bramy
Ports: At_Attacker: 20(4), 21(1), 25(1) At_Victim: 23(1)

ID: 52.130655 Date: 04/06/1999 Name: pod Category: dos
Start Time: 13:06:00 Duration: 00:00:30 Attacker: 166.102.114.043
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: 80(1)

ID: 52.132827 Date: 04/06/1999 Name: New Attack '1999 (yaga)
Category: u2r Start Time: 13:28:11 Duration: 00:42:19
Attacker: 194.007.248.153 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 23(2), 30(1)

ID: 52.135003 Date: 04/06/1999 Name: cramilis Category: dos
Start Time: 13:50:03 Duration: 00:00:05 Attacker: 194.007.248.153
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 80(1)

ID: 52.140207 Date: 04/06/1999 Name: New Attack '99 (ppmmacro)
Category: r21 Start Time: 14:26:26 Duration: 00:12:52
Attacker: 199.174.194.016 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: 137/u(1) At_Victim: i(1), 25(1), 80(12)

ID: 52.141200 Date: 04/06/1999 Name: syslogd Category: dos
Start Time: 14:13:56 Duration: 00:00:01 Attacker: 172.003.045.001
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: 514/u(1)
ID: 52.142452 Date: 04/06/1999 Name: perl Category: u2r
Start_Time: 14:24:17 Duration: 00:14:47 Attacker: 207.103.080.104
Victim: 172.016.114.207 Username: gregors
Ports: At_Attacker: At_Victim: 23[1]

ID: 52.162435 Date: 04/06/1999 Name: fdformat Category: u2r
Start_Time: 16:24:15 Duration: 01:00:00 Attacker: 196.038.075.158
Victim: 172.016.112.250 Username: victors janelles
Ports: At_Attacker: At_Victim: 20[5], 21[1], 23[1]

ID: 52.165435 Date: 04/06/1999 Name: queso Category: probe
Start_Time: 16:54:20 Duration: 00:00:51 Attacker: 199.227.099.125
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: At_Victim: 25[7]

ID: 52.181637 Date: 04/06/1999 Name: Neptune Category: dos
Start_Time: 18:16:05 Duration: 00:03:26 Attacker: 010.020.030.040
Victim: 192.168.001.001 Username: n/a
Ports: At_Attacker: At_Victim: 1-1024[10]

ID: 52.205605 Date: 04/06/1999 Name: New Attack 1999 (dosnuko)
Category: dos Start_Time: 20:57:03 Duration: 00:01:33
Attacker: 172.016.115.234 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 139[1]

ID: 52.211313 Date: 04/06/1999 Name: ipsweep Category: probe
Start_Time: 21:15:54 Duration: 00:19:30 Attacker: 195.073.151.050
Ports: At_Attacker: At_Victim: 80[195]

ID: 52.214522 Date: 04/06/1999 Name: ncftp Category: r2t
Start_Time: 21:45:02 Duration: 00:01:28 Attacker: 172.016.118.020
Victim: 172.016.114.050 Username: bramy anonymous

ID: 52.2050813 Date: 04/07/1999 Name: udpstorm Category: dos
Start_Time: 05:30:38 Duration: 00:00:01 Attacker: 172.016.112.050
Victim: 172.016.113.* Username: n/a
Ports: At_Attacker: At_Victim: 7/u[1]

ID: 53.045454 Date: 04/08/1999 Name: selfping Category: dos
Start_Time: 05:04:19 Duration: 00:01:02 Attacker: 135.008.060.182
Victim: 172.016.112.050 Username: bramy
Ports: At_Attacker: At_Victim: 23[1]

ID: 53.084346 Date: 04/07/1999 Name: xlock Category: r2t
Start_Time: 08:46:02 Duration: 00:00:25 Attacker: 152.204.242.193
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker:  At_Victim: 6000(1)
ID: 53.085717 Date: 04/07/1999 Name: php Category: r21
Start_Time: 08:58:16 Duration: 00:00:01 Attacker: 209.001.012.046
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker:  At_Victim: 80(1)
ID: 53.092039 Date: 04/07/1999 Name: New Attack 1999 (tcpreset)
Category: probe Start_Time: 09:44:00 Duration: 00:15:00
Attacker: hobbes_console Victim: 172.016.112.050
Username: n/a
Ports: At_Attacker:  At_Victim: 
ID: 53.094800 Date: 04/07/1999 Name: New Attack 1999 (netbus)
Category: r21 Start_Time: 09:50:33 Duration: 02:14:28
Attacker: 209.167.099.071 Victim: 172.016.112.100
Username: Path:
Ports: At_Attacker:  At_Victim: 25(1), 12345-12346(1)
ID: 53.102617 Date: 04/07/1999 Name: back Category: dos
Start_Time: 10:26:12 Duration: 00:00:04 Attacker: 152.204.242.193
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker:  At_Victim: 80(40)
ID: 53.110500 Date: 04/07/1999 Name: New Attack 1999 (netcat)
Category: r21 Start_Time: 11:06:56 Duration: 00:30:11
Attacker: 172.016.113.084 Victim: 197.182.091.233 Username: n/a
Ports: At_Attacker:  At_Victim: 25(1)
ID: 53.110516 Date: 04/07/1999 Name: queso Category: probe
Start_Time: 11:32:16 Duration: 00:13:05 Attacker: 197.182.091.233
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker:  At_Victim: 23(7)
ID: 53.123735 Date: 04/07/1999 Name: portsweep Category: probe
Start_Time: 12:37:10 Duration: 00:09:32 Attacker: 204.097.153.043
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker:  At_Victim: 1[2], 2-6[1], 7[2], 8[1], 9[2], 10[1]
ID: 53.133203 Date: 04/07/1999 Name: perl Category: u2r
Start_Time: 13:33:17 Duration: 00:10:46 Attacker: 209.017.189.098
Victim: 172.016.112.207 Username: doireano argument
/home/doireano/NewProjects/Working/Solaris/Chuck/rlogin.c
Ports: At_Attacker:  At_Victim: 23(1)
ID: 53.134015 Date: 04/07/1999 Name: queso Category: probe
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker:  At_Victim: 25(7)
ID: 53.144800 Date: 04/07/1999 Name: snmpget Category: r21
Start_Time: 14:49:35 Duration: 00:01:45 Attacker: 207.230.054.203
Victim: 172.016.000.001 Username: n/a
Ports: At_Attacker:  At_Victim: 161/u[21]
ID: 53.150110 Date: 04/07/1999 Name: processtable Category: dos
Start Time: 15:01:16 Duration: 00:31:05 Attacker: 172.016.117.052
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: 25(378)

ID: 53.152648 Date: 04/07/1999 Name: back Category: dos
Start Time: 15:26:15 Duration: 00:01:49 Attacker: 194.027.251.021
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 80(40)

ID: 53.155432 Date: 04/07/1999 Name: fbconfig Category: u2r
Start Time: 16:05:00 Duration: 06:45:59 Attacker: 195.115.218.108
Victim: 172.016.112.050 Username: bellej tristank karstenf
Ports: At_Attacker: 23(1), 25(1)

ID: 53.171350 Date: 04/07/1999 Name: apache2 Category: dos
Start Time: 17:13:17 Duration: 00:08:39 Attacker: 172.016.117.052
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: 80(412)

ID: 53.195130 Date: 04/07/1999 Name: portswEEP Category: probe
Start Time: 19:51:19 Duration: 00:01:48 Attacker: 209.030.071.165
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: 1-52(1), 54-100(1)

ID: 54.082003 Date: 04/08/1999 Name: ps Category: u2r
Start Time: 08:33:00 Duration: 00:03:00 Attacker: console
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim:

ID: 54.090101 Date: 04/08/1999 Name: psf Category: r2l
Start Time: 09:01:08 Duration: 00:31:46 Attacker: 206.048.044.050
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 80(8)

ID: 54.091200 Date: 04/08/1999 Name: New Attack 1999 {casesen}
Category: u2r Start Time: 09:16:20 Duration: 02:03:47
Attacker: 172.016.112.149 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 20(4), 21(1), '23(2)

ID: 54.102102 Date: 04/08/1999 Name: New Attack 1999 {ntfSdos}
Category: r2l Start Time: 10:21:00 Duration: 00:15:00
Attacker: 172.16.112.100 Victim: 172.16.112.100 Username: n/a
Ports: At_Attacker: At_Victim: i(1)

ID: 54.103459 Date: 04/08/1999 Name: portswEEP Category: probe
Start Time: 10:34:11 Duration: 00:05:44 Attacker: 153.010.008.174
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 22(1), 79(1), 514(1)

ID: 54.110416 Date: 04/08/1999 Name: ntinfoscan Category: probe
Start Time: 11:26:37 Duration: 00:16:09 Attacker: 206.048.044.018
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 20-21(1), 23(1), 80(11), 139(2)

ID: 54.115000 Date: 04/08/1999 Name: New Attack 1999 {yaga}
Category: u2r Start Time: 11:52:05 Duration: 00:15:39

149
attacker: 194.007.248.153 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 23[2], 80[1]

D: 54.115701 Date: 04/08/1999 Name: crashhiis Category: dos
Start Time: 11:57:01 Duration: 00:00:03 Attacker: 194.007.248.153
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 80[1]

D: 54.120600 Date: 04/08/1999 Name: http_tunnel Category: r21
Start Time: 12:06:30 Duration: 00:03:31 Attacker: 172.016.112.050
Victim: 196.037.075.158 Username: n/a
Ports: At_Attacker: At_Victim: 8000[9]

D: 54.125758 Date: 04/08/1999 Name: idformat Category: u2r
Start Time: 12:57:17 Duration: 00:40:10 Attacker: 194.027.251.021
Victim: 172.016.112.050 Username: doireano valeskad emerye eberharm rodolph
Ports: At_Attacker: At_Victim: 20-21[1], 23[1]

D: 54.145832 Date: 04/08/1999 Name: satan Category: probe
Start Time: 14:58:29 Duration: 00:02:12 Attacker: 209.074.060.168
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 1-9999[1], 1/u-1303/u[1]

ID: 54.155338 Date: 04/08/1999 Name: teardrop Category: dos
Start Time: 15:53:18 Duration: 00:00:01 Attacker: 199.227.099.125
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 23/u[1]

ID: 54.160341 Date: 04/08/1999 Name: New_Attack_1999 (sechole)
Category: u2r Start Time: 16:03:15 Duration: 00:21:56
Attacker: 208.240.124.083 Victim: 172.016.112.100 Username: ansgarz
Ports: At_Attacker: At_Victim: 20[2], 21[1], 23[2]

ID: 54.170132 Date: 04/08/1999 Name: resetscan Category: probe
Start Time: 17:01:19 Duration: 00:01:02 Attacker: 172.016.117.103
Victim: 172.016.112.* Username: n/a
Ports: At_Attacker: At_Victim: 21[1]

ID: 54.171643 Date: 04/08/1999 Name: ipsweep Category: probe
Start Time: 17:16:10 Duration: 00:01:31 Attacker: 172.016.112.005, 172.016.112.010, 207.136.086.223 Victim: 172.016.112.001-010, 207.136.086.223 Username: n/a
Ports: At_Attacker: At_Victim: i[2] At_Victim: i[10]

ID: 54.175007 Date: 04/08/1999 Name: snmpget Category: r21
Start Time: 17:50:12 Duration: 00:05:06 Attacker: 194.027.251.021
Victim: 172.016.000.001 Username: n/a
Ports: At_Attacker: At_Victim: 161/u[61]

ID: 54.183002 Date: 04/08/1999 Name: ntinfoscan Category: probe
Start Time: 18:31:00 Duration: 00:16:11 Attacker: 206.048.044.018
Victim: 172.016.111.100 Username: n/a
Ports: At_Attacker: At_Victim: 20-21[1], 23[31], 80[11], 139[2]

ID: 54.190707 Date: 04/08/1999 Name: New_Attack_1999 (ls)
Category: probe Start Time: 19:08:31 Duration: 00:00:01

150
Attacker: 209.012.013.144  Victim: 172.016.112.020  Username: n/a
Ports: At_Attacker:  At_Victim: 53(1)

ID: 54.194108  Date: 04/08/1999  Name: New_Attack_1999 (warezclient)
Category: dos  Start_Time: 19:41:14  Duration: 00:00:41
Attacker: 209.030.070.014  Victim: 172.016.112.050  Username: n/a
Ports: At_Attacker:  At_Victim: 20-21(1)

ID: 54.195951  Date: 04/09/1999  Name: mscan  Category: probe
Start_Time: 19:58:59  Duration: 04:03:05  Attacker: 207.136.086.223
Victim: 172.016.112.010, 172.016.112.020, 172.016.112.050,
172.016.112.100, 172.016.112.149, 172.016.112.194, 172.016.112.207,
172.016.113.050, 172.016.113.084, 172.016.113.105, 172.016.113.204,
172.016.115.005, 172.016.115.087, 172.016.115.234, 172.016.116.044,
172.016.117.11, 172.016.117.132, 172.016.118.010, 172.016.118.020,
172.016.118.030, 172.016.118.040, 172.016.118.050, 172.016.118.060,
172.016.118.070, 172.016.118.080, 172.016.118.090, 172.016.118.100
Username: n/a
Ports: At_Attacker:  At_Victim: 23[32], 25[16], 79-80[16], 110[48],
111[15], 143[16], 6000[16]

ID: 54.225131  Date: 04/11/1999  Name: New_Attack_1999 (arppoisoin)
Category: probe  Start_Time: 22:51:14  Duration: 00:28:01
Attacker: 135.013.216.191  Victim: 172.016.112.100  Username: abramh
Ports: At_Attacker:  At_Victim: 23(1)

ID: 55.080105  Date: 04/09/1999  Name: portsweep  Category: probe
Start_Time: 00:01:28  Duration: 00:00:29  Attacker: 172.016.113.050
Victim: 206.048.044.050  Username: n/a
Ports: At_Attacker:  At_Victim: 34904[1], 49826[1], 50460[1]

ID: 55.080500  Date: 04/09/1999  Name: xsnoop  Category: r2l
Start_Time: 00:08:37  Duration: 00:01:19  Attacker: 194.027.251.021
Victim: 172.016.113.050  Username: n/a
Ports: At_Attacker:  At_Victim: 6000[1]

ID: 55.081418  Date: 04/09/1999  Name: crashiis  Category: dos
Start_Time: 08:14:17  Duration: 00:00:45  Attacker: 172.016.117.11
Victim: 172.016.112.100  Username: n/a
Ports: At_Attacker:  At_Victim: 80[1]

ID: 55.082500  Date: 04/09/1999  Name: New_Attack_1999 (illegalsniffer)
Category: probe  Start_Time: 08:26:21  Duration: 00:17:53
Attacker: 172.016.112.098  Victim: 172.016.112.*  Username: n/a
Ports: At_Attacker:  At_Victim: 

ID: 55.084452  Date: 04/09/1999  Name: back  Category: dos
Start_Time: 08:44:16  Duration: 00:01:49  Attacker: 206.047.098.151
Victim: 172.016.114.050  Username: n/a
Ports: At_Attacker:  At_Victim: 80[40]

ID: 55.085500  Date: 04/09/1999  Name: New_Attack_1999 (illegalsniffer)
Category: probe  Start_Time: 08:53:46  Duration: 00:25:58
Attacker: 172.016.112.097  Victim: 172.016.112.*  Username: n/a
Ports: At_Attacker:  At_Victim: 

151


ID: 55.100600 Date: 04/09/1999 Name: anypw Category: r21 Start Time: 10:45:00 Duration: 00:15:00 Attacker: 172.16.112.100 Victim: 172.16.112.100 Username: n/a Ports: At_Attacker: At_Victim: 25(1)

ID: 55.100830 Date: 04/09/1999 Name: guest Category: r21 Start Time: 10:08:13 Duration: 00:00:52 Attacker: 172.016.118.050 Victim: 172.016.112.050 Username: guest Ports: At_Attacker: At_Victim: 23(9)

ID: 55.102000 Date: 04/09/1999 Name: New_Attack_1999 (tcpreset) Category: probe Start Time: 10:20:00 Duration: 00:05:00 Attacker: hobses_console Victim: 172.016.112.100 Username: n/a Ports: At_Attacker: At_Victim:

ID: 55.103001 Date: 04/09/1999 Name: perl Category: u2r Start Time: 10:35:00 Duration: 00:05:00 Attacker: console Victim: 172.016.114.050 Username: n/a Ports: At_Attacker: At_Victim:


ID: 55.123412 Date: 04/09/1999 Name: sqlattack Category: r21 Start Time: 12:34:15 Duration: 00:01:02 Attacker: 206.186.080.111 Victim: 172.016.112.194 Username: db3 Ports: At_Attacker: At_Victim: 23(1)

ID: 55.124400 Date: 04/09/1999 Name: New Attack 1999 (yaga) Category: u2r Start Time: 12:44:38 Duration: 00:17:42 Attacker: 209.001.012.046 Victim: 172.016.112.100 Username: n/a Ports: At_Attacker: At_Victim: 23(2), 80(2)

ID: 55.125112 Date: 04/09/1999 Name: crashihs Category: dos
Start Time: 12:51:12 Duration: 00:00:32 Attacker: 209.001.012.046
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 80(1)

ID: 55.125811 Date: 04/09/1999 Name: guesstelnet Category: r2l
Start Time: 12:58:11 Duration: 00:10:05 Attacker: 135.013.216.191
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 23(20)

ID: 55.125830 Date: 04/09/1999 Name: crashiis Category: dos
Start Time: 12:58:30 Duration: 00:00:03 Attacker: 209.001.012.046
Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 80(1)

ID: 55.140643 Date: 04/09/1999 Name: syslogd Category: dos
Start Time: 14:06:15 Duration: 00:00:01 Attacker: 172.005.004.066
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 514/u(1)

ID: 55.141732 Date: 04/09/1999 Name: eject Category: u2r
Start Time: 14:17:28 Duration: 00:04:18 Attacker: 206.048.044.050
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 20-21[1], 23[1]

ID: 55.163447 Date: 04/09/1999 Name: land Category: dos
Start Time: 14:32:27 Duration: 00:00:01 Attacker: 172.016.113.050
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: At_Victim: 25[1]

ID: 55.171917 Date: 04/09/1999 Name: syslogd Category: dos
Start Time: 14:56:30 Duration: 00:00:01 Attacker: 172.005.004.065
Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 514/u(1)

ID: 55.172757 Date: 04/09/1999 Name: sendmail Category: r2l
Start Time: 17:27:15 Duration: 00:00:11 Attacker: 152.204.242.193
Victim: 172.016.114.050 Username: n/a
Ports: At_Attacker: At_Victim: 25[1]

ID: 55.174733 Date: 04/09/1999 Name: xterm Category: u2r
Start Time: 17:47:15 Duration: 00:37:40 Attacker: 202.072.001.077
Ports: At_Attacker: At_Victim: 20(2), 21[1], 23[1]

ID: 55.183012 Date: 04/09/1999 Name: Neptune Category: dos
Start Time: 18:30:04 Duration: 00:00:09 Attacker: 011.021.031.041
Victim: 172.016.113.050 Username: n/a
Ports: At_Attacker: At_Victim: 21(400)

ID: 55.184715 Date: 04/09/1999 Name: perl Category: u2r
Start Time: 18:47:14 Duration: 00:35:49 Attacker: 172.016.112.194
Victim: 172.016.114.050 Username: yuvalt Name
Ports: At_Attacker: At_Victim: 23[1]

ID: 55.185233 Date: 04/09/1999 Name: New_Attack_1999 (warexclient)
Category: dos Start Time: 18:52:09 Duration: 00:00:41
Attacker: 206.047.098.151 Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim: 20-21(1)

ID: 55.202002 Date: 04/09/1999 Name: queso Category: probe
Start_Time: 20:20:20 Duration: 00:18:07 Attacker: 205.160.208.190
Victim: 172.016.000.001 Username: n/a
Ports: At_Attacker: At_Victim: 80(7)

ID: 55.204925 Date: 04/09/1999 Name: Now Attack 1999 {caseness}
Category: u2r Start_Time: 20:49:17 Duration: 00:43:47
Attacker: 204.071.051.016 Victim: 172.016.112.100 Username: n/a
Ports: At_Attacker: At_Victim: 20[3], 21[1], 23[2]

ID: 55.200530 Date: 04/09/1999 Name: New Attack 1999 {secret}
Category: data Start_Time: 20:05:30 Duration: 00:10:00
Attacker: console Victim: 172.016.112.050 Username: n/a
Ports: At_Attacker: At_Victim:
Appendix E: Snort Rule sets

Snort 1.7 Full Ruleset

# http://www.snort.org Snort 1.7 Rule set
# Contact: snort-sigs@lists.sourceforge.net
# NOTE: This rule set only works for 1.7.0 and later

include local.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
include telnet.rules
include smtp.rules
include rpc.rules
include rservices.rules
include backdoor.rules
include dos.rules
include ddos.rules
include dns.rules
include netbios.rules
include sql.rules
include web-cqi.rules
include web-coldfusion.rules
include web-frontpage.rules
include web-misc.rules
include web-iis.rules
include icmp.rules
include misc.rules
include policy.rules
include info.rules
include virus.rules

Snort 1.7 Custom Rule set

# http://www.snort.org Snort 1.7 Rule set
# Contact: snort-sigs@lists.sourceforge.net
# NOTE: This rule set only works for 1.7.0 and later

include local.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
include telnet.rules
include smtp.rules
include rpc.rules
include rservices.rules
include backdoor.rules
include dos.rules
include ddos.rules
include dns.rules
include netbios.rules
include sql.rules
include web-cqi.rules
include web-coldfusion.rules
include web-frontpage.rules
include web-misc.rules
include web-iis.rules
include icmp.rules
include misc.rules
include policy.rules
# include info.rules
include virus.rules

Snort 1.8.3 Full Ruleset
#---------------------------------------------------------------
# http://www.snort.org Snort 1.8.1 Ruleset
# Contact: snort-sigs@lists.sourceforge.net
#---------------------------------------------------------------
# NOTE: This ruleset only works for 1.8.0 and later
#---------------------------------------------------------------
# $Id: snort.conf,v 1.79 2002/01/02 16:12:54 cazz Exp $
#---------------------------------------------------------------
include bad-traffic.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
include telnet.rules
include smtp.rules
include rpc.rules
include rservices.rules
include dos.rules
include ddos.rules
include dns.rules
include tftp.rules
include web-cgi.rules
include web-coldfusion.rules
include web-frontpage.rules
include web-iis.rules
include web-misc.rules
include web-attacks.rules
include sql.rules
include xll.rules
include icmp.rules
include netbios.rules
include misc.rules
include attack-responses.rules
include backdoor.rules
include shellcode.rules
include policy.rules
include porn.rules
include info.rules
# include icmp-info.rules
include virus.rules
include experimental.rules
include local.rules

Snort 1.8.3 Custom Ruleset:
#---------------------------------------------------------------
# http://www.snort.org Snort 1.8.1 Ruleset
# Contact: snort-sigs@lists.sourceforge.net
#---------------------------------------------------------------
# NOTE: This ruleset only works for 1.8.0 and later
include bad-traffic.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
include telnet.rules
include smtp.rules
include rpc.rules
include rservices.rules
include dos.rules
include ddos.rules
include dns.rules
include tftp.rules
include web-cgi.rules
include web-coldfusion.rules
include web-frontpage.rules
include web-iis.rules
include web-misc.rules
include web-attacks.rules
include sql.rules
include xll.rules
include icmp.rules
include netbios.rules
include misc.rules
include attack-responses.rules
# include backdoor.rules
# include shellcode.rules
# include policy.rules
# include porn.rules
# include info.rules
# include icmp-info.rules
# include virus.rules
# include experimental.rules
include local.rules
### Appendix F: Result Form for Test Data Set 1

<table>
<thead>
<tr>
<th>Week</th>
<th>Day</th>
<th>Attack Category</th>
<th>Attack Name</th>
<th>Snort 1.7 Full</th>
<th>Snort 1.7 Custom</th>
<th>Snort 1.8 Full</th>
<th>Snort 1.8 Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Mon</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mon</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mon</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Tues</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Wed</td>
<td>DoS</td>
<td>Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Ffb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>R2L</td>
<td>Dict</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>U2R</td>
<td>Ffb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Thurs</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td>Time</td>
<td>Attack</td>
<td>Target</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>thurs</td>
<td>U2R</td>
<td>Perlmagic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Perlmagic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Ftb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix G: Result Form for Test Data Set 2

<table>
<thead>
<tr>
<th>Week</th>
<th>Day</th>
<th>Attack Category</th>
<th>Attack Name</th>
<th>Snort 1.7 Full</th>
<th>Snort 1.7 Custom</th>
<th>Snort 1.8 Full</th>
<th>Snort 1.8 Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Mon</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>DoS</td>
<td>Syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mon</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>Probe</td>
<td>Portswipe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>U2R</td>
<td>Ffb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tues</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Wed</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>U2R</td>
<td>Loadmodule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>Probe</td>
<td>Portswipe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>U2R</td>
<td>Perlmagic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Thurs</td>
<td>DoS</td>
<td>Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix H: Result Form for Test Data set 3

<table>
<thead>
<tr>
<th>Week</th>
<th>Day</th>
<th>Attack Category</th>
<th>Attack Name</th>
<th>Snort 1.7 Full</th>
<th>Snort 1.7 Custom</th>
<th>Snort 1.8 Full</th>
<th>Snort 1.8 Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mon</td>
<td>U2R</td>
<td>Ps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Sendmail</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>U2R</td>
<td>Ntfsdos</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>Probe</td>
<td>Portswep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Ssh trojan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>Probe</td>
<td>Portswep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Xsnoop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Snmp get</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>G ess telnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>Probe</td>
<td>Portswep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Guess ftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>R2L</td>
<td>Ftp write</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>U2R</td>
<td>Yaga</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>DoS</td>
<td>Crashii</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>Probe</td>
<td>Portswep</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>Data</td>
<td>Secret</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mon</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>R2L</td>
<td>Http tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>R2L</td>
<td>Pf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>U2R</td>
<td>Loadmod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>U2R</td>
<td>Ps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>U2R</td>
<td>Ntfs dos</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>Data</td>
<td>Secret</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>R2L</td>
<td>Sql attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>U2R</td>
<td>Se ch o le</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>DoS</td>
<td>Mail bomb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>DoS</td>
<td>Pro cess tab le</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Tues</td>
<td>DoS</td>
<td>Crash ii</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>R2L</td>
<td>Net cat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>R2L</td>
<td>Imap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>R2L</td>
<td>Ppmacro</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>DoS</td>
<td>Pro cess tab le</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>U2R</td>
<td>Fd format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>R2L</td>
<td>Ne break in</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Weds</td>
<td>DoS</td>
<td>W ar e</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td>Time</td>
<td>Attack</td>
<td>Tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>---------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>R2L</td>
<td>Arppoison</td>
<td>Neftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>Data</td>
<td>Secret</td>
<td>Named</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>R2L</td>
<td>Named</td>
<td>Guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>DoS</td>
<td>Smurf</td>
<td>Guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>Probe</td>
<td>Portsweep</td>
<td>Guesstelnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>DoS</td>
<td>Mailbomb</td>
<td>Snmpget</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weds</td>
<td>R2L</td>
<td>Teardrop</td>
<td>Ncftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Netbus</td>
<td>Ppmarco</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Sshtrajan</td>
<td>Guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Dosnuka</td>
<td>Xlock</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Ncftp</td>
<td>Guesspop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Phf</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Processtable</td>
<td>Sqlattack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Mailbomb</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Sqlattack</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Smurf</td>
<td>Probe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Arppoison</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Sshtrajan</td>
<td>Probe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Ipsweep</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Xlock</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Named</td>
<td>Probe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Portsweep</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Netbus</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Mailbomb</td>
<td>Probe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Ipsweep</td>
<td>U2R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Loadmod</td>
<td>Sechole</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Sechole</td>
<td>Probe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Portsweep</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Data</td>
<td>Secret</td>
<td>R2L</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appendix I: Result Form for Test Data Set 4

<table>
<thead>
<tr>
<th>Week</th>
<th>Day</th>
<th>Attack Category</th>
<th>Attack Name</th>
<th>Snort 1.7 Full</th>
<th>Snort 1.7 Custom</th>
<th>Snort 1.8 Full</th>
<th>Snort 1.8 Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>WarzeLient</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Apache2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>R2L</td>
<td>GuessStelnEt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>DosnUKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>U2R</td>
<td>Loadmodule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>U2R</td>
<td>FibConFig</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Smurf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>ArpPoiSon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Apache2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>R2L</td>
<td>Imap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>Probe</td>
<td>IpswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>R2L</td>
<td>Dict</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>SyslogD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>CrashIis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>Probe</td>
<td>Ls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>DosnUKE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>UdpStorm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>DoS</td>
<td>SelfPing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mon</td>
<td>R2L</td>
<td>Ncftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>DoS</td>
<td>TepresEt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>U2R</td>
<td>Casesen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>R2L</td>
<td>Xsnoop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>DoS</td>
<td>SelfPing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>U2R</td>
<td>Xterm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>R2L</td>
<td>FtpWrite</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>DoS</td>
<td>Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>U2R</td>
<td>Ps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tues</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td>Time</td>
<td>Tool</td>
<td>Command</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>R2L</td>
<td>Http_tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>DoS</td>
<td>Pod</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>U2R</td>
<td>Yaga</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>DoS</td>
<td>Crashii_s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>R2L</td>
<td>Ppmacro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>DoS</td>
<td>Syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>U2R</td>
<td>Perl</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>U2R</td>
<td>Fdformat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>Data</td>
<td><em>secret</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>Probe</td>
<td>Qeso</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>DoS</td>
<td>Dosnuke</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tues</td>
<td>R2L</td>
<td>Neftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Udpstorm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Selfping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>R2L</td>
<td>Xlock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Tcepreset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>R2L</td>
<td>Netbus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>R2L</td>
<td>Netcat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>Probe</td>
<td>Qeso</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>U2R</td>
<td>Perl</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>Probe</td>
<td>Qeso</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>R2L</td>
<td>Snmpget</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Processstable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>U2R</td>
<td>Ffbconfig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>DoS</td>
<td>Apache2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wed</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Ps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Phf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Casesen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Ntfsdos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>PortswEEP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Ntunfoscan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Yaga</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Crashii_s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Http_tunnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Fdformat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Satan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Teardrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td>Time</td>
<td>Command</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>U2R</td>
<td>Sechole</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Resetscan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Ipsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>R2L</td>
<td>Snmpget</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Ntinfoscan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Ls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Warezclient</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>Probe</td>
<td>Mscan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thurs</td>
<td>DoS</td>
<td>Arppoison</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>portsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Xsnoop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Crashiis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Insidesniffer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Netcat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Xterm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>portsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Anypw</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Tepreset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Perl</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Framespoofer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>portsweep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Sqlattack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Yaga</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Crashiis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Guesstelnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Crashiis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Syslogd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Eject</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Land</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Syslogd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>R2L</td>
<td>Sendmail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Xterm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Neptune</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Perl</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>DoS</td>
<td>Warezclient</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Probe</td>
<td>Queso</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>U2R</td>
<td>Casesen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fri</td>
<td>Data</td>
<td>Secret</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix J: Sample Snort Configuration File

#------------------------------------------------------
# http://www.snort.org  Snort 1.7 Ruleset
# Contact: snort-sigs@lists.sourceforge.net:
#------------------------------------------------------
# NOTE:This ruleset only works for 1.7 and later
#------------------------------------------------------
# $Id: snort.conf,v 1.110 2002/08/14 03:17:58 chrisgreen Exp $
#
# You must change the following variables to reflect
# your local network.
#
# You can specify it explicitly as:
#
# var HOME_NET 10.1.1.0/24
#
# or use global variable $<interfacename> ADDRESS
# which will be always initialized to IP address and
# netmask of the network interface which you run
# snort at.
#
# var HOME_NET $eth0 ADDRESS
#
# You can specify lists of IP addresses for HOME_NET
# by separating the IPs with commas like this:
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:
var HOME_NET $eth0 ADDRESS
#
# Set up the external network addresses as well.
# A good start may be "any"
var EXTERNAL_NET !$HOME_NET
#
# Configure your server lists. This allows snort to only look for attacks
# to systems that have a service up. Why look for HTTP attacks if you are
# not running a web server? This allows quick filtering based on IP addresses
# These configurations MUST follow the same configuration scheme as defined
# above for $HOME_NET.
#
# List of DNS servers on your network
var DNS_SERVERS $HOME_NET
#
# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET
#
# List of web servers on your network
var HTTP_SERVERS $HOME_NET
#
# List of sql servers on your network
var SQL_SERVERS $HOME_NET

# List of telnet servers on your network
var TELNET_SERVERS $HOME_NET

# Configure your service ports. This allows snort to look for attacks
# destined to a specific application only on the ports that application
# runs on. For example, if you run a web server on port 8081, set your
# HTTP_PORTS variable like this:
#
# var HTTP_PORTS 8081
#
# Port lists must either be continuous [eg 80:8080], or a single port [eg 80].
# We will adding support for a real list of ports in the future.
#
# Ports you run web servers on
var HTTP_PORTS 80
#
# Ports you want to look for SHELLCODE on.
var SHELLCODE_PORTS 180
#
# Ports you do oracle attacks on
var ORACLE_PORTS 1521
#
# other variables
#
# Path to your rules files (this can be a relative path)
var RULE_PATH $IDS_BASE/rules

# General configuration for preprocessors is of
# the form
# preprocessor <name_of_processor>: <configuration_options>
# frag2: IP defragmentation support
# -----------------------------------------------
# This preprocessor performs IP defragmentation. This plugin will also detect
# people launching fragmentation attacks (usually DoS) against hosts. No
# arguments loads the default configuration of the preprocessor, which is a
# 60 second timeout and a 4MB fragment buffer.
# The following (comma delimited) options are available for frag2
# timeout [seconds] - sets the number of [seconds] than an unfinished
# fragment will be kept around waiting for completion,
# if this time expires the fragment will be flushed
# memcap [bytes] - limit frag2 memory usage to [number] bytes
# (default: 4194304)
# min_ttl [number] - minimum ttl to accept
# ttl_limit [number] - difference of ttl to accept without alerting
# will cause false positives with router flap
#
# Frag2 uses Generator ID 113 and uses the following SIDS
# for that GID:
# SID    Event description
# -----  -------------------
# 1  Oversized fragment (reassembled frag > 64k bytes)
# 2  Teardrop-type attack
#
# preprocessor frag2
#
# stream4: stateful inspection/stream reassembly for Snort

167
Use in concert with the -z [all|est] command line switch to defeat
stick/snot against TCP rules. Also performs full TCP stream
assembly, stateful inspection of TCP streams, etc. Can statefully
detect various portsscan types, fingerprinting, ECN, etc.

# stateful inspection directive
# no arguments loads the defaults (timeout 30, memcap 8388608)
# options (options are comma delimited):
  detect_scans - stream4 will detect stealth ports scans and generate alerts
  when it sees them when this option is set
  detect_state_problems - detect TCP state problems, this tends to be very
  noisy because there are a lot of crappy ip stack
  implementations out there

  disable_evasion_alerts - turn off the possibly noisy mitigation of
  overlapping sequences.

  min_ttl [number] - set a minimum ttl that snort will accept to
  stream reassembly

  ttl_limit [number] - differential of the initial ttl on a session
  versus
  the normal that someone may be playing games.
  Routing flap may cause lots of false positives.

  keepstats [machine|binary] - keep session statistics, add "machine" to
  get them in a flat format for machine reading, add
  "binary" to get them in a unified binary output
  format

  noinspect - turn off stateful inspection only

  timeout [number] - set the session timeout counter to [number] seconds,
  default is 30 seconds

  memcap [number] - limit stream4 memory usage to [number] bytes

  log_flushed_streams - if an event is detected on a stream this option will
  cause all packets that are stored in the stream4
  packet buffers to be flushed to disk. This only
  works when logging in pcap mode!

# Stream4 uses Generator ID 111 and uses the following SIDS
# for that GID:

<table>
<thead>
<tr>
<th>SID</th>
<th>Event description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stealth activity</td>
</tr>
<tr>
<td>2</td>
<td>Evasive RST packet</td>
</tr>
<tr>
<td>3</td>
<td>Evasive TCP packet retransmission</td>
</tr>
<tr>
<td>4</td>
<td>TCP Window violation</td>
</tr>
<tr>
<td>5</td>
<td>Data on SYN packet</td>
</tr>
<tr>
<td>6</td>
<td>Stealth scan: full XMAS</td>
</tr>
<tr>
<td>7</td>
<td>Stealth scan: SYN-ACK-PSH-URG</td>
</tr>
<tr>
<td>8</td>
<td>Stealth scan: FIN scan</td>
</tr>
<tr>
<td>9</td>
<td>Stealth scan: NULL scan</td>
</tr>
<tr>
<td>10</td>
<td>Stealth scan: NMAP XMAS scan</td>
</tr>
<tr>
<td>11</td>
<td>Stealth scan: Vecna scan</td>
</tr>
<tr>
<td>12</td>
<td>Stealth scan: NMAP fingerprint scan stateful detect</td>
</tr>
<tr>
<td>13</td>
<td>Stealth scan: SYN-FIN scan</td>
</tr>
<tr>
<td>14</td>
<td>TCP forward overlap</td>
</tr>
</tbody>
</table>

preprocessor stream4

# tcp stream reassembly directive
# no arguments loads the default configuration
Only reassemble the client.
Only reassemble the default list of ports (See below).
Give alerts for "bad" streams

Available options (comma delimited):
clientonly - reassemble traffic for the client side of a connection only
serveronly - reassemble traffic for the server side of a connection only
both - reassemble both sides of a session
noalerts - turn off alerts from the stream reassembly stage of stream4
ports [list] - use the space separated list of ports in [list], "all"
            will turn on reassembly for all ports, "default" will turn
            on reassembly for ports 21, 23, 25, 53, 80, 143, 110, 111
            and 513

preprocessor stream4_reassemble
 # http_decode: normalize HTTP requests
    # http_decode normalizes HTTP requests from remote
    # machines by converting any %XX character
    # substitutions to their ASCII equivalent. This is
    # very useful for doing things like defeating hostile
    # attackers trying to stealth themselves from IDSs by
    # mixing these substitutions in with the request.
    # Specify the port numbers you want it to analyze as arguments.
 # Major code cleanups thanks to rfp
 #
 # unicode - normalize unicode
 # iis_alt_unicode = \u encoding from iis
 # double_encode - alert on possible double encodings
 # iis_flip_slash - normalize \ as /
 # full_whitespace - treat \t as whitespace ( for apache )
 #
 # for that GID:
 # SID     Event description
 #-------    ------------------
 #  1     UNICODE attack
 #  2     NULL byte attack

preprocessor http_decode: 80 unicode iis_alt_unicode double_encode
                        iis_flip_slash full_whitespace
 # rpc_decode: normalize RPC traffic
    # RPC may be sent in alternate encodings besides the usual
    # 4-byte encoding that is used by default. This preprocessor
    # normalized RPC traffic in much the same way as the http_decode
    # preprocessor. This plugin takes the ports numbers that RPC
    # services are running on as arguments.
    # The RPC decode preprocessor uses generator 1D 106 and does not
    # generate any SIDs at this time.

preprocessor rpc_decode: 111 32771
 # bo: Back Orifice detector
    # Detects Back Orifice traffic on the network. This preprocessor
    # uses the Back Orifice "encryption" algorithm to search for
    # traffic conforming to the Back Orifice protocol (not BO2K).
    # This preprocessor can take two arguments. The first is 
    # "-nobrute" which turns off the plugin's brute forcing routine (brute forces
    # the key space of the protocol to find BO traffic). The second
# argument that can be passed to the routine is a number to use
# as the default key when trying to decrypt the traffic. The
# default value is 31337 (just like BO). Be aware that turning on
# the brute forcing option runs the risk of impacting the overall
# performance of Snort, you've been warned...

# The Back Orifice detector uses Generator ID 105 and uses the
# following SIDS for that GID:
# SID Event description
# ---- ----------------
# 1 Back Orifice traffic detected

preprocessor bo: -nobrute 10

# telnet_decode: Telnet negotiation string normalizer
# ---------------------------------------------------------------------
# This preprocessor "normalizes" telnet negotiation strings from
# telnet and ftp traffic. It works in much the same way as the
# http decode preprocessor, searching for traffic that breaks up
# the normal data stream of a protocol and replacing it with
# a normalized representation of that traffic so that the "context-
# pattern matching keyword can work without requiring modifications.
# This preprocessor requires no arguments.
# Portscan uses Generator ID 109 and does not generate any SID currently.

preprocessor telnet_decode

# Portscan: detect a variety of portscans
# ---------------------------------------
# portscan preprocessor by Patrick Mullen <p_mullen@linuxrc.net>
# This preprocessor detects UDP packets or TCP SYN packets going to
# four different ports in less than three seconds. "Stealth" TCP
# packets are always detected, regardless of these settings.
# Portscan uses Generator ID 100 and uses the following SIDS for that GID:
# SID Event description
# ---- ----------------
# 1 Portscan detect
# 2 Inter-scan info
# 3 Portscan End

preprocessor portscan: $HOME_NET 5 3 $LOGDIR/$INSTANCE.scan

# Use portscan-ignorehosts to ignore TCP SYN and UDP "scans" from
# specific networks or hosts to reduce false alerts. It is typical:
# to see many false alerts from DNS servers so you may want to
# add your DNS servers here. You can all multiple hosts/networks
# in a whitespace-delimited list.

preprocessor portscan-ignorehosts: 0.0.0.0

# arpspoof
# --------------------------------------
# Experimental ARP detection code from Jeff Nathan, detects ARP attacks,
# unicast ARP requests, and specific ARP mapping monitoring. To make use
# of this preprocessor you must specify the IP and hardware address of hosts on
# the same layer 2 segment as you. Specify one host IP MAC combo per line.
# Also takes a "unicast" option to turn on unicast ARP request detection.
# Arpspoof uses Generator ID 112 and uses the following SIDS for that GID:
# SID Event description
# ---- ----------------
# 1 Unicast ARP request
# 2 Etherframe ARP mismatch (src)
# 3 Etherframe ARP mismatch (dst)
# 4 ARP cache overwrite attack

170
preprocessor arpspoof
preprocessor arpspoof_detect_host: f0:0f:00:f0:0f:00

# ASN1 Decode
#--------------------------------------------------
# This is an experimental preprocessor. ASN.1 decoder and analysis plugin
# from Andrew R. Baker. This preprocessor will detect abuses of the ASN.1
# protocol that higher level protocols (like SSL, SNMP, x.509, etc) rely on.
# The ASN.1 decoder uses Generator ID 115 and uses the following SIDs for
# that GID:
# SID  Event description
#-----  ------------------
# 1  Indefinite length
# 2  Invalid length
# 3  Oversized item
# 4  ASN.1 specification violation
# 5  Dataum bad length

preprocessor asn1_decode

# Fnord
#--------------------------------------------------
# This is an experimental preprocessor. Polymorphic shellcode analyzer and
# detector by Dragos Ruiu. This preprocessor will watch traffic for
# polymorphic NOP-type sleds to defeat tools like ADMutate. The Fnord detector
# uses Generator ID 114 and the following SIDs:
# SID  Event description
#-----  ------------------
# 1  NOP-sled detected

preprocessor fnord

# Conversation
#--------------------------------------------------
# This preprocessor tracks conversations for tcp, udp and icmp traffic. It
# is a prerequisite for running portscan2.
# allowed_ip_protocols 1 6 17
# list of allowed ip protocols (defaults to any)
# timeout [num]
# conversation timeout ( defaults to 60 )
# max_conversations [num]
# number of conversations to support at once (defaults to 65335)
# alert_odd_protocols
# alert on protocols not listed in allowed_ip_protocols

preprocessor conversation: allowed_ip_protocols all, timeout 60,
max_conversations 32000

# Portscan2
#--------------------------------------------------
# Portscan 2, detect portscans in a new and exciting way.
# Available options:
# scanners_max [num]
# targets_max [num]
# target_limit [num]
# port_limit [num]
# timeout [num]
# log [logdir]

preprocessor portscan2: scanners_max 3200, targets max 5000, target_limit 5, port_limit 20, timeout 60
# Experimental Perf stats
# ------------------------
# No docs. Highly subject to change.
# preprocessor perfmonitor: console flow events time 10

#########################################################################
# Uncomment and configure the output plugins you decide to use.       #
# General configuration for output plugins is of the form:             #
# output <name_of_plugin>: <configuration_options>                    #
# alert_syslog: log alerts to syslog                                   #
# Use one or more syslog facilities as arguments                     #
# output alert_syslog: LOG_LOCAL5 LOG_ALERT                           #
# log_tcpdump: log packets in binary tcpdump format                   #
# The only argument is the output file name.                          #
# output log_tcpdump: <$INSTANCE>                                     #
### output alert_fast: $INSTANCE.alert                               #
### output alert_full: $INSTANCE.alert                               #
###
# database: alert
# -----------------------------------------------
# See the README.database file for more information about configuring  #
# and using this plugin.                                             #
# output database: alert                                             #
# output database: alert, postgresql, user=snort dbname=snort         #
# output database: log, unixodbc, user=snort dbname=snort             #
# output database: log, mysql, dbname=snort user=snort password=test  #
# xml: xml logging
# -------------------------------------------------------
# See the README.xml file for more information about configuring       #
# and using this plugin.                                             #
# output xml: log, file=$foo/bar cert=foo port=3 protocol=http         #

# unified: Snort unified binary format alerting and logging
# -----------------------------------------------------------
# The unified output plugin provides two new formats for logging     #
# and generating alerts from Snort, the "unified"-format. The        #
# unified format is a straight binary format for logging data        #
# out of Snort that is designed to be fast and efficient. Used with  #
# barnyard (the new alert/log processor), most of the overhead       #
# for logging and alerting to various slow storage mechanisms
such as databases or the network can now be avoided.

Two arguments are supported.

- **filename** - base filename to write to (current time is appended)
- **limit** - maximum size of spool file in MB (default: 128)

Output alert Unified: filename $LOGDIR/$INSTANCE-alert.uni, limit 128
Output log Unified: filename $LOGDIR/$INSTANCE-log.uni, limit 128

# trap_snmp: SNMP alerting for Snort

-------------------------------

Read the README.SNMP file for more information on enabling and using this plug-in.

# The trap_snmp plugin accepts the following notification options

- **c**: Generate compact notifications. (Saves on bandwidth by not reporting MOs for which values are unknown, not available or, not applicable). By default this option is reset.
- **p**: Generate a print of the invariant part of the offending packet. This can be used to track the packet across the Internet.
- **m**: Use the MD5 algorithm to generate the packet print. By default this algorithm is used.
- **s**: Use the SHA1 algorithm to generate the packet print.

The trap_snmp plugin requires several parameters

The parameters depend on the SnmpVersion that is used (specified)

For the SNMPv2c case the parameters will be as follows

- **alert**, <sensorID>, [NotificationOptions],
- **(trap|inform) -v <SnmpVersion> -p <portNumber> <hostName> <community>

For SNMPv2c traps with MD5 digest based packetPrint generation

- **output trap_snmp: alert, 7, cpm, trap -v 2c myTrapListener myCommunity**

For SNMPv2c informs with the 'compact' notification option

- **output trap_snmp: alert, 7, c, inform -v 2c myTrapListener myCommunity**

For SNMPv3 traps with

- **security name = snortUser**
- **security level = authentication and privacy**
- **authentication parameters**
  - authentication protocol = SHA
  - authentication pass phrase = SnortAuthPassword
- **privacy (encryption) parameters**
  - privacy protocol = DES
  - privacy pass phrase = SnortPrivPassword

- **output trap_snmp: alert, 7, trap -v 3 -u snortUser -l authPriv -a SHA -A SnortAuthPassword -x DES -x SnortPrivPassword myTrapListener**

- **For SNMPv3 informs with authentication and encryption**
- **output trap_snmp: alert, 7, inform -v 3 -u snortUser -l authPriv -a SHA -A SnortAuthPassword -x DES -x SnortPrivPassword myTrapListener**

# You can optionally define new rule types and associate one or
# more output plugins specifically to that type.
# This example will create a type that will log to just tcpdump.
ruletype suspicious
{
type log
output log_tcdump: suspicious.log
}

# EXAMPLE RULE FOR SUSPICIOUS RULETYPE:
suspicious $HOME_NET any -> $HOME_NET 6667 (msg:"Internal IRC Server");

ruletype redalert
{
type alert
output alert_syslog: LOG_LOCAL5 LOG_ALERT
output database: alert
}

# EXAMPLE RULE FOR REDALERT RULETYPE
redalert $HOME_NET any -> $EXTERNAL_NET 31337 (msg:"Someone is being LEET"; flags:A+;)

# Include classification & priority settings

include $IDS_BASE/etc/classification.config
include $IDS_BASE/etc/redalert.config

# Include reference systems

include $IDS_BASE/etc/reference.config

*****************************************************************************
# Up to date snort rules are available at http://www.snort.org
#
# The snort web site has documentation about how to write your own
# custom snort rules.
#
# The rules included with this distribution generate alerts based on
# suspicious activity. Depending on your network environment, your
# security policies, and what you consider to be suspicious, some of
# these rules may either generate false positives or may be detecting
# activity you consider to be acceptable; therefore, you are
# encouraged to comment out rules that are not applicable in your
# environment.
#
# Note that using all of the rules at the same time may lead to
# serious packet loss on slower machines. YMMV, use with caution,
# standard disclaimers apply. :)
#
# The following individuals contributed many of the rules in this
# distribution.
#
# Credits:
#    Ron Gula <rgula@securitywizards.com> of Network Security Wizards
#    Max Vision <vision@whitehats.com>
#    Martin Markgraf <martin@mail.dtu.tn.com>
#    Fyodor Yarochkin <fygrave@tigerteam.net>
# include all relevant rulesets here

# shellcode, policy, info, backdoor, and virus rulesets are
disabled by default. These require tuning and maintenance.
# Please read the included specific file for more information.

include local.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
include telnet.rules
include smtp.rules
include rpc.rules
include rservices.rules
include backdoor.rules
include dos.rules
include ddos.rules
include dns.rules
include netbios.rules
include sql.rules
include web-cgi.rules
include web-coldfusion.rules
include web-frontpage.rules
include web-misc.rules
include web-iis.rules
include icmp.rules
include misc.rules
include policy.rules
include info.rules
include virus.rules