nfdump and NfSen

18th Annual FIRST Conference
June 25-30, 2006 Baltimore
Peter Haag
nfdump and NfSen

Some operational questions, popping up now and then:

• Do you see this peek on port 445 as well?
• What caused this peek on your network graph?
• How did SoberR spread in your network?
• Do we have any traffic pattern of this incident?
• Which host/subnet consumes most of your bandwidth?
• Which are the top talkers in your network?
• …

Sober.R
nfdump and NfSen

How to find answers for all these questions?

Netflow turns out to be a good Data Source - although not the only one - for all kind of information and/or events to look at.

.. in discussions with other teams:
   – “Watch your flows for …”
   – “I’ve seen a lot of … in our flows …”
   – “Hosts are infected, when you see flows to …”
nfdump and NfSen

What is NetFlow?

_NetFlow is a traffic monitoring technology developed by Cisco Networks. Flows are unidirectional and contain connection related data such as:_

- Source and destination IP address.
- Source and destination port.
- Source and destination AS.
- Level3 protocol, ToS byte, TCP flags.
- Logical input and output interfaces.
- Bytes and packet counters.

Example:


Netflow records never contain any user data!
How to get netflow data and how to look at them?

Routers do provide netflow data …

but …

Router# show ip cache flow

… seems not to be the solution for every task.

⇒ Tools to collect and look at the netflow data

nfdump and NfSen
nfdump and NfSen:

**NfSen:**
- Web based frontend
- Display flows
- Framework to automate tasks

**nfdump:**
- Collect and store flows
- Process flows on command line
nfdump and NfSen

nfdump overview:

- netflow v5, v7 or v0 exporter
- sflow exporter
- nfcapd
- sfcapd
- storage
- nfdump

Collecting data

Processing data

Text

Binary

nfcapd.2006xx
nfdump and NfSen

nfdump features:

• CMD line based tool comparable to tcpdump.
• Written in C ⇒ fast.
• Stores netflow data in time sliced files.
• Supports netflow format v5, v7 and v9.
• Supports sflow.
• All processing options support IPv4 and IPv6.
• Powerful pcap like filter syntax:
  ( proto tcp and dst net 172.16/16 and src port > 1024 and bytes < 600 )
  or ( bps > 1k and …
• Flexible flow aggregation: srcip,dstip,srcport,dstport,srcas,dstas,proto
• Efficient filter engine: > 6 Mio flows/s on 3GHz Intel.
• Lots of fast Top N statistics.
• Anonymizing of IP addresses. ( Crypto-Pan )
• User defined output formats.
Example:

List the first 20 tcp flows:

```
fenth% nfdump -r /data/rz/nfcapd.200603300150 -K 123.. -c 20 ‘proto tcp’
```

<table>
<thead>
<tr>
<th>Date</th>
<th>Flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-03-30</td>
<td>00:43:40.569</td>
<td>82.880</td>
<td>TCP</td>
<td>130.20.234.125:58035 -&gt;</td>
<td>200.66.27.5:61486</td>
<td>.AP...</td>
<td>673</td>
<td>199208</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:43:40.569</td>
<td>82.880</td>
<td>TCP</td>
<td>200.66.27.5:61486 -&gt;</td>
<td>130.20.234.125:58035</td>
<td>.A.....</td>
<td>421</td>
<td>19674</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:44:00.082</td>
<td>63.113</td>
<td>TCP</td>
<td>130.20.234.125:55697 -&gt;</td>
<td>159.93.88.3:60454</td>
<td>.AP...</td>
<td>814</td>
<td>1.1 M</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:44:00.082</td>
<td>63.113</td>
<td>TCP</td>
<td>159.93.88.3:60454 -&gt;</td>
<td>130.20.234.125:55697</td>
<td>.A.....</td>
<td>498</td>
<td>25896</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.647</td>
<td>0.431</td>
<td>TCP</td>
<td>193.246.238.35:80 -&gt;</td>
<td>192.254.4.182:56547</td>
<td>.A.....</td>
<td>1</td>
<td>1500</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.647</td>
<td>0.431</td>
<td>TCP</td>
<td>192.254.4.182:56547 -&gt;</td>
<td>193.246.238.35:80</td>
<td>.A.....</td>
<td>3</td>
<td>156</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.813</td>
<td>0.000</td>
<td>TCP</td>
<td>130.20.234.124:59112 -&gt;</td>
<td>194.50.123.176:45458</td>
<td>.A...F</td>
<td>1</td>
<td>52</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.913</td>
<td>0.000</td>
<td>TCP</td>
<td>192.254.4.167:58659 -&gt;</td>
<td>49.20.115.83:80</td>
<td>.A...F</td>
<td>1</td>
<td>52</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.913</td>
<td>0.000</td>
<td>TCP</td>
<td>129.66.105.181:11248 -&gt;</td>
<td>192.254.4.183:80</td>
<td>...S.</td>
<td>1</td>
<td>46</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.913</td>
<td>0.000</td>
<td>TCP</td>
<td>192.254.4.183:80 -&gt;</td>
<td>129.66.105.181:11248</td>
<td>.A..S.</td>
<td>1</td>
<td>46</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.879</td>
<td>0.000</td>
<td>TCP</td>
<td>129.66.105.181:11247 -&gt;</td>
<td>192.254.4.183:80</td>
<td>.A.....</td>
<td>1</td>
<td>515</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.879</td>
<td>0.000</td>
<td>TCP</td>
<td>192.254.4.183:80 -&gt;</td>
<td>129.66.105.181:11247</td>
<td>.A.....</td>
<td>1</td>
<td>46</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.913</td>
<td>0.355</td>
<td>TCP</td>
<td>214.203.35.177:19027 -&gt;</td>
<td>130.20.234.125:80</td>
<td>.A.....</td>
<td>3</td>
<td>156</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>01:40:02.347</td>
<td>300.572</td>
<td>TCP</td>
<td>dffe:e6...199:fd.119 -&gt;</td>
<td>dc7e:18...fe99:2.35541</td>
<td>.AP...</td>
<td>811</td>
<td>66835</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>01:40:02.347</td>
<td>300.572</td>
<td>TCP</td>
<td>dc7e:18...fe99:2.35541 -&gt;</td>
<td>dffe:e6...199:fd.119</td>
<td>.AP...S</td>
<td>4850</td>
<td>6.9 M</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.895</td>
<td>0.000</td>
<td>TCP</td>
<td>192.254.4.183:80 -&gt;</td>
<td>192.254.179.207:56323</td>
<td>.AP...</td>
<td>1</td>
<td>129</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:02.978</td>
<td>0.000</td>
<td>TCP</td>
<td>194.50.123.176:45465 -&gt;</td>
<td>130.20.234.124:55652</td>
<td>...S.</td>
<td>1</td>
<td>60</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:03.013</td>
<td>0.000</td>
<td>TCP</td>
<td>130.20.234.125:21</td>
<td>50.242.99.240:61288</td>
<td>.A..S.</td>
<td>1</td>
<td>48</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:03.009</td>
<td>0.000</td>
<td>TCP</td>
<td>156.32.82.45:35110</td>
<td>130.20.234.124:25</td>
<td>...S.</td>
<td>1</td>
<td>60</td>
</tr>
<tr>
<td>2006-03-30</td>
<td>00:45:03.041</td>
<td>0.000</td>
<td>TCP</td>
<td>130.20.234.125:80</td>
<td>130.219.188.88:57168</td>
<td>.A.....</td>
<td>1</td>
<td>52</td>
</tr>
</tbody>
</table>

IP addresses anonymized

Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:10

Total flows: 15970 matched: 20, skipped: 0, Bytes read: 838972
Sys: 0.007s flows/second: 2044290.8 Wall: 0.004s flows/second: 3391378.2
**Example:**

Show the top 15 IP addresses consuming most bandwidth:

`forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123... -n 20 -s ip/bps`

Top 15 IP Addr ordered by bps:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>IP Addr</th>
<th>Flows</th>
<th>Packets</th>
<th>Bytes</th>
<th>pps</th>
<th>bps</th>
<th>bpp</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-03-30 00:47:39.999</td>
<td>0.001 TCP</td>
<td>64.132.143.51</td>
<td>2</td>
<td>19</td>
<td>18004</td>
<td>18999</td>
<td>137.4 M</td>
<td>947</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:45:00.737</td>
<td>0.001 TCP</td>
<td>194.64.105.184</td>
<td>2</td>
<td>20</td>
<td>13600</td>
<td>20000</td>
<td>103.8 M</td>
<td>680</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:49:16.016</td>
<td>0.001 TCP</td>
<td>163.3.33.241</td>
<td>2</td>
<td>9</td>
<td>12046</td>
<td>9000</td>
<td>91.9 M</td>
<td>1338</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:49:52.902</td>
<td>0.001 TCP</td>
<td>92.37.170.104</td>
<td>2</td>
<td>10</td>
<td>9208</td>
<td>10000</td>
<td>70.3 M</td>
<td>920</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:45:06.853</td>
<td>0.001 TCP</td>
<td>214.214.200.81</td>
<td>2</td>
<td>6</td>
<td>6931</td>
<td>6000</td>
<td>52.9 M</td>
<td>1155</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:46:32.363</td>
<td>0.001 TCP</td>
<td>68.142.57.84</td>
<td>2</td>
<td>10</td>
<td>6720</td>
<td>10000</td>
<td>51.3 M</td>
<td>672</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:46:30.764</td>
<td>0.001 TCP</td>
<td>151.80.146.115</td>
<td>2</td>
<td>7</td>
<td>6680</td>
<td>7000</td>
<td>51.0 M</td>
<td>954</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:48:36.966</td>
<td>0.001 TCP</td>
<td>129.4.38.113</td>
<td>2</td>
<td>8</td>
<td>6184</td>
<td>8000</td>
<td>47.2 M</td>
<td>773</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:49:31.903</td>
<td>0.001 TCP</td>
<td>33.135.213.117</td>
<td>2</td>
<td>6</td>
<td>6104</td>
<td>6000</td>
<td>46.6 M</td>
<td>1017</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:42:46.834</td>
<td>0.001 TCP</td>
<td>90.38.160.152</td>
<td>2</td>
<td>8</td>
<td>5941</td>
<td>8000</td>
<td>45.3 M</td>
<td>742</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:48:02.473</td>
<td>0.001 TCP</td>
<td>131.144.55.170</td>
<td>2</td>
<td>6</td>
<td>5608</td>
<td>6000</td>
<td>42.8 M</td>
<td>934</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:49:29.424</td>
<td>0.001 TCP</td>
<td>24.11.195.220</td>
<td>2</td>
<td>4</td>
<td>4880</td>
<td>4000</td>
<td>37.2 M</td>
<td>1220</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:48:53.293</td>
<td>0.001 TCP</td>
<td>88.53.69.175</td>
<td>2</td>
<td>6</td>
<td>4721</td>
<td>6000</td>
<td>36.0 M</td>
<td>786</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 00:45:41.780</td>
<td>0.001 TCP</td>
<td>49.30.8.60</td>
<td>2</td>
<td>6</td>
<td>3822</td>
<td>6000</td>
<td>29.2 M</td>
<td>637</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:42:51.618</td>
<td>0.002 TCP</td>
<td>220.24.222.74</td>
<td>2</td>
<td>10</td>
<td>7605</td>
<td>5000</td>
<td>29.0 M</td>
<td>760</td>
<td></td>
</tr>
</tbody>
</table>

IP addresses anonymized

Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58

Total flows: 19224 matched: 19224, skipped: 0, Bytes read: 1009920

Sys: 0.046s flows/second: 410112.0 Wall: 0.009s flows/second: 222089.0
nfdump and NfSen

Example:
Show port scanning candidates:

`forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123... -A srcip,dstport -s record/packets 'not proto icmp and bytes < 100 and bpp < 100 and packets < 5 and not port 80 and not port 53 and not port 110 and not port 123'

Aggregated flows 72506
Top 10 flows ordered by packets:

<table>
<thead>
<tr>
<th>Date</th>
<th>flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>bps</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-03-30 01:49:23.800</td>
<td>243.842 TCP</td>
<td>83.130.48.231:0</td>
<td>-&gt;</td>
<td>0.0.0.0:4899</td>
<td>142172</td>
<td>6.5 M</td>
<td>223891</td>
<td>71151</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:50:48.603</td>
<td>236.035 TCP</td>
<td>165.17.105.18:0</td>
<td>-&gt;</td>
<td>0.0.0.0:5900</td>
<td>34452</td>
<td>1.6 M</td>
<td>56049</td>
<td>17232</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:52:30.169</td>
<td>143.944 TCP</td>
<td>117.128.149.163:0</td>
<td>-&gt;</td>
<td>0.0.0.0:41523</td>
<td>9982</td>
<td>479136</td>
<td>26629</td>
<td>5143</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:49:22.650</td>
<td>303.173 TCP</td>
<td>221.200.120.170:0</td>
<td>-&gt;</td>
<td>0.0.0.0:1433</td>
<td>4638</td>
<td>222624</td>
<td>5874</td>
<td>2319</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:49:53.945</td>
<td>299.401 TCP</td>
<td>211.135.150.43:0</td>
<td>-&gt;</td>
<td>0.0.0.0:135</td>
<td>3273</td>
<td>157104</td>
<td>4197</td>
<td>3273</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:52:05.471</td>
<td>96.768 TCP</td>
<td>198.246.113.17:0</td>
<td>-&gt;</td>
<td>0.0.0.0:445</td>
<td>1678</td>
<td>80544</td>
<td>6658</td>
<td>954</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:49:22.970</td>
<td>328.838 TCP</td>
<td>201.143.63.114:0</td>
<td>-&gt;</td>
<td>0.0.0.0:139</td>
<td>1845</td>
<td>88560</td>
<td>3641</td>
<td>1613</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:52:05.471</td>
<td>96.768 TCP</td>
<td>198.246.113.17:0</td>
<td>-&gt;</td>
<td>0.0.0.0:445</td>
<td>1678</td>
<td>80544</td>
<td>6658</td>
<td>954</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:49:54.012</td>
<td>300.038 UDP</td>
<td>210.117.33.36:0</td>
<td>-&gt;</td>
<td>0.0.0.0:137</td>
<td>1471</td>
<td>114738</td>
<td>3059</td>
<td>1471</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:49:22.970</td>
<td>328.838 TCP</td>
<td>164.88.206.114:0</td>
<td>-&gt;</td>
<td>0.0.0.0:135</td>
<td>1432</td>
<td>68736</td>
<td>1672</td>
<td>1077</td>
<td></td>
</tr>
<tr>
<td>2006-03-30 01:53:00.822</td>
<td>112.524 TCP</td>
<td>24.169.235.184:0</td>
<td>-&gt;</td>
<td>0.0.0.0:135</td>
<td>1254</td>
<td>60192</td>
<td>4279</td>
<td>1254</td>
<td></td>
</tr>
</tbody>
</table>

IP addresses anonymized
Time window: 2006-03-30 01:34:53 - 2006-03-30 01:54:57
Total flows: 1178835 matched: 245494, skipped: 0, Bytes read: 57559680
Sys: 0.634s flows/second: 1856716.7 Wall: 0.632s flows/second: 1862657.6
nfdump and NfSen

Example:
Show the top 15 /24 subnets exchanging most traffic:

```bash
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123... -n 15 -A srcip4/24,dstip4/24 -s record/bytes
```

Aggregated flows 7525

Top 15 flows ordered by bytes:

<table>
<thead>
<tr>
<th>Date flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-03-30 00:41:06.140</td>
<td>4102.844</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 130.254.221.0:0</td>
<td>79455</td>
<td>95.1 M</td>
<td>14</td>
</tr>
<tr>
<td>2006-03-30 00:42:50.622</td>
<td>4022.361</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 194.90.158.0:0</td>
<td>42179</td>
<td>58.2 M</td>
<td>13</td>
</tr>
<tr>
<td>2006-03-30 00:40:51.729</td>
<td>4054.221</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 220.63.34.0:0</td>
<td>39593</td>
<td>56.0 M</td>
<td>6</td>
</tr>
<tr>
<td>2006-03-30 01:41:42.025</td>
<td>443.957</td>
<td>TCP</td>
<td>130.254.221.0:0</td>
<td>-&gt; 130.20.234.0:0</td>
<td>60178</td>
<td>29.1 M</td>
<td>14</td>
</tr>
<tr>
<td>2006-03-30 01:39:56.087</td>
<td>600.881</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 194.84.7.0:0</td>
<td>17836</td>
<td>24.9 M</td>
<td>9</td>
</tr>
<tr>
<td>2006-03-30 00:44:39.128</td>
<td>3900.855</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 214.124.39.0:0</td>
<td>15912</td>
<td>22.6 M</td>
<td>9</td>
</tr>
<tr>
<td>2006-03-30 01:41:01.414</td>
<td>529.568</td>
<td>UDP</td>
<td>130.20.223.0:0</td>
<td>-&gt; 130.20.220.0:0</td>
<td>15549</td>
<td>21.4 M</td>
<td>8</td>
</tr>
<tr>
<td>2006-03-30 01:41:03.371</td>
<td>329.612</td>
<td>TCP</td>
<td>194.114.160.0:0</td>
<td>-&gt; 130.20.234.0:0</td>
<td>14126</td>
<td>20.1 M</td>
<td>4</td>
</tr>
<tr>
<td>2006-03-30 01:40:12.986</td>
<td>300.997</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 194.168.190.0:0</td>
<td>13101</td>
<td>18.7 M</td>
<td>2</td>
</tr>
<tr>
<td>2006-03-30 01:41:24.088</td>
<td>506.896</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 24.50.25.0:0</td>
<td>12433</td>
<td>17.8 M</td>
<td>2</td>
</tr>
<tr>
<td>2006-03-30 01:43:04.047</td>
<td>300.870</td>
<td>TCP</td>
<td>165.242.80.0:0</td>
<td>-&gt; 130.20.234.0:0</td>
<td>9966</td>
<td>14.3 M</td>
<td>1</td>
</tr>
<tr>
<td>2006-03-30 00:43:47.441</td>
<td>3935.542</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 205.175.61.0:0</td>
<td>10445</td>
<td>13.4 M</td>
<td>15</td>
</tr>
<tr>
<td>2006-03-30 00:44:01.619</td>
<td>332.758</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 194.61.253.0:0</td>
<td>8973</td>
<td>12.7 M</td>
<td>101</td>
</tr>
<tr>
<td>2006-03-30 01:42:43.123</td>
<td>300.860</td>
<td>TCP</td>
<td>130.20.234.0:0</td>
<td>-&gt; 69.155.45.0:0</td>
<td>7872</td>
<td>11.3 M</td>
<td>1</td>
</tr>
</tbody>
</table>

IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58
Total flows: 19224 matched: 18797, skipped: 0, Bytes read: 1009920
Sys: 0.062s flows/second: 307588.9 Wall: 0.010s flows/second: 1839969.4
nfdump and NfSen

The art of filter design:

• ... depends on your problem you want to look at.
  – Incident Analysis.
  – Host tracking.
  – Port Scanning.
  – Operational issues.

• ... depends on your network.

nfump does not do your job, but supports you in doing your job!

Use the power of nfdump’s filter syntax!
nfdump and NfSen

nfdump is:
• Powerful
• Flexible
• Easy to use
• Fast
• ...

but ...

... don't we all like pictures?

⇒ NfSen
nfdump and NfSen

NfSen features:

• Use the power of nfdump as backend tool. ⇒ modular design.
• Pictures!
• Drill down from overview to the details down to the specific flows.
• Graph current network situation.
• Graph specific profiles.
  – Track hosts, ports etc. from live data.
  – Profile hosts involved in incidents from history data.
• Analyse a specific time window.
• Web based.
• Automatically post process netflow data for reporting and alerting purpose.
• Flexible extensions using plugins.
• Easy to use.
• Auto - Cleanup. Aging data files: max space, max lifetime.
nfdump and NfSen

Putting all together:

- Input
  - netflow v5, v7, v9, sflow

- nfdump Backend
  - nfdump

- Web Front-end
  - softflowd
  - pfflowd

- Post Processing
  - Periodic Update Tasks & Plugins

- CLI
nfdump and NfSen

Overview ⇒ Details

Details ⇒ Flows
### NFSEN – Profile live May 01 2006 – 21:30

**Profile: live**

**TCP** | **any** | **ICMP** | **other**
--- | --- | --- | ---
![Graphs](image)

**Profileinfo:**
- **Type:** continuous
- **Max:** unlimited
- **Exp:** never
- **Start:** Apr 02 2006 - 01:15
- **End:** May 03 2006 - 09:30

**Mon May 1 21:30:00 2006 Packets/s proto UDP**

**Flows**

**Traffic**

**Statistics timeslot May 01 2006 - 21:30**

<table>
<thead>
<tr>
<th>Source</th>
<th>Flows:</th>
<th>Packets:</th>
<th>Traffic:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all:</td>
<td>tcp:</td>
<td>udp:</td>
</tr>
<tr>
<td>All</td>
<td>509.9 K/s</td>
<td>10.1 K/s</td>
<td>8.2 K/s</td>
</tr>
<tr>
<td>Downstream</td>
<td>6.1 K/s</td>
<td>126.9 K/s</td>
<td>112.1 K/s</td>
</tr>
<tr>
<td>Upstream</td>
<td>3.9 K/s</td>
<td>448.6 K/s</td>
<td>436.9 K/s</td>
</tr>
<tr>
<td>Peer1</td>
<td>3.5 K/s</td>
<td>48.0 K/s</td>
<td>40.4 K/s</td>
</tr>
<tr>
<td>Peer2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Display:**
- Sum
- Rate
Profile: live

TCP  any  ICMP  other

Profile info:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:18
End: May 03 2006 - 09:30

Tue May 2 04:55:00 2006 Packets/s proto UDP

Select  left  Mark  Display:  1 day  <<  <  |  >  >>  >1

Statistics timeslot May 02 2006 - 04:55

<table>
<thead>
<tr>
<th>Source</th>
<th>Flows:</th>
<th>Packets:</th>
<th>Traffic:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all</td>
<td>tcp</td>
<td>udp</td>
</tr>
<tr>
<td>Downstream</td>
<td>506.6 K/s</td>
<td>3.3 K/s</td>
<td>2.7 K/s</td>
</tr>
<tr>
<td>Upstream</td>
<td>4.1 K/s</td>
<td>182.3 K/s</td>
<td>39.3 K/s</td>
</tr>
<tr>
<td>Peer1</td>
<td>3.0 K/s</td>
<td>350.6 K/s</td>
<td>344.5 K/s</td>
</tr>
<tr>
<td>Peer2</td>
<td>2.4 K/s</td>
<td>22.4 K/s</td>
<td>18.7 K/s</td>
</tr>
<tr>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Netflow Processing

#### Source:
- **Downstream**
- **Upstream**
- **Peer1**
- **Peer2**

#### Filter:
- **udp**

#### Show:
- **List:** First
- **Stat:** Top

---

```
Aggregated flows 23100
Top 20 flows ordered by packets:
```

<table>
<thead>
<tr>
<th>Date flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Flags</th>
<th>Dst IP Addr:Port</th>
<th>Port</th>
<th>Bytes</th>
<th>pps</th>
<th>bps</th>
<th>bps Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-05-02 04:43:47.315</td>
<td>3.1900 s</td>
<td>UDP</td>
<td>254.118.64.166:7001</td>
<td>31919</td>
<td>190.50.223.175:7000</td>
<td>0</td>
<td>4.7 M</td>
<td>36</td>
<td>45282</td>
<td>153</td>
</tr>
<tr>
<td>2006-05-02 04:43:47.339</td>
<td>3.1900 s</td>
<td>UDP</td>
<td>190.50.223.175:7000</td>
<td>26147</td>
<td>254.118.64.166:7000</td>
<td>0</td>
<td>3.9 M</td>
<td>30</td>
<td>34574</td>
<td>155</td>
</tr>
<tr>
<td>2006-05-02 04:43:47.256</td>
<td>3.1900 s</td>
<td>UDP</td>
<td>247.3.328.90:7000</td>
<td>18676</td>
<td>247.3.328.90:7000</td>
<td>2</td>
<td>2.6 M</td>
<td>26</td>
<td>32777</td>
<td>159</td>
</tr>
<tr>
<td>2006-05-02 04:43:47.287</td>
<td>3.1900 s</td>
<td>UDP</td>
<td>924.588:102.128:6380</td>
<td>67380</td>
<td>191.181.110.74:8350</td>
<td>0</td>
<td>1.8 M</td>
<td>24</td>
<td>23112</td>
<td>119</td>
</tr>
</tbody>
</table>

---

```
IP addresses anonymized
Flows analysed: 151994 matched: 29565, bytes read: 7431168
Sys: 0.066 s flows/second: 2338765.0 Wall: 0.061 s flows/second: 2474988.6
```
Profile: live

TCP  any  ICMP  other

Fri Apr 21 08:20:00 2006 Packets/s proto UDP

Select  left  Mark  Display:  12 Hours  <<  <  >  >>

Statistics timeslot Apr 21 2006 - 03:20

<table>
<thead>
<tr>
<th>Source</th>
<th>Flow</th>
<th>Packets:</th>
<th>Traffic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downstream</td>
<td>all: 212.3/s</td>
<td>tcp: 2.7/s</td>
<td>icmp: 625.0/s</td>
</tr>
<tr>
<td>Upstream</td>
<td>all: 4.2 K/s</td>
<td>tcp: 728.0 K/s</td>
<td>icmp: 958.6 Mbs</td>
</tr>
<tr>
<td>Peer1</td>
<td>all: 2.6 K/s</td>
<td>tcp: 761.0 K/s</td>
<td>icmp: 932.9 Mbs</td>
</tr>
<tr>
<td>Peer2</td>
<td>all: 2.1 K/s</td>
<td>tcp: 472.8 K/s</td>
<td>icmp: 811.8 Mbs</td>
</tr>
</tbody>
</table>

Netflow Processing
Netflow Processing

Source: Filter:
- Downstream
- Upstream
- Peer1
- Peer2

Show:
- List: First
  - 10 Flows
    - aggregated
    - time sorted
    - long output

Stat: Top
- 20 Flows
  - Packets
  - order by bps
  - long output
- ANY IP Addr

Clear Form

```
```

Aggregated flows 1090426
Top 20 flows ordered by bps:

<table>
<thead>
<tr>
<th>Date</th>
<th>Flow start</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Tos</th>
<th>Packets</th>
<th>Bytes</th>
<th>pps</th>
<th>bps</th>
<th>Bps Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006-04-21</td>
<td>03:17:04.531</td>
<td>456.636s</td>
<td>UDP</td>
<td>171.232.166.244:37623</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>129.4 M</td>
<td>5.8 G</td>
<td>29725</td>
<td>104.3 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:04.738</td>
<td>460.499s</td>
<td>UDP</td>
<td>123.46.184.211:47125</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>129.8 M</td>
<td>5.8 G</td>
<td>294944</td>
<td>103.5 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:05.121</td>
<td>232.128s</td>
<td>UDP</td>
<td>171.8.244.170:46294</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>32.2 M</td>
<td>1.4 G</td>
<td>155543</td>
<td>51.1 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:06.123</td>
<td>236.096s</td>
<td>UDP</td>
<td>126.205.7.190:67018</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>32.5 M</td>
<td>1.5 G</td>
<td>144085</td>
<td>50.6 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:06.152</td>
<td>328.128s</td>
<td>UDP</td>
<td>108.44.41.181:5830</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>32.3 M</td>
<td>1.5 G</td>
<td>103351</td>
<td>36.3 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:08.122</td>
<td>356.224s</td>
<td>UDP</td>
<td>109.93.137.123:45644</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>32.1 M</td>
<td>1.4 G</td>
<td>94634</td>
<td>33.1 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:17:08.396</td>
<td>552.256s</td>
<td>UDP</td>
<td>119.137.230.210:4537</td>
<td>253.163.140.151:53</td>
<td>......</td>
<td>0</td>
<td>32.0 M</td>
<td>1.4 G</td>
<td>80795</td>
<td>21.3 M</td>
<td>46</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:20:23.378</td>
<td>0.001 UDP</td>
<td>15.238.99.170:5</td>
<td>191.196.25.129:32899</td>
<td>0</td>
<td>6</td>
<td>1878</td>
<td>6000</td>
<td>16.3 M</td>
<td>313</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:20:35.152</td>
<td>0.001 UDP</td>
<td>179.216.81.1:53</td>
<td>252.152.125.20:32769</td>
<td>0</td>
<td>6</td>
<td>1110</td>
<td>6000</td>
<td>16.3 M</td>
<td>313</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:22:25.250</td>
<td>0.001 UDP</td>
<td>106.230.159.83:53</td>
<td>253.227.215.30529</td>
<td>0</td>
<td>6</td>
<td>1040</td>
<td>8000</td>
<td>7.9 M</td>
<td>130</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:23:06.113</td>
<td>0.001 UDP</td>
<td>193.32.20.52:5</td>
<td>253.227.215.30279</td>
<td>0</td>
<td>129</td>
<td>24</td>
<td>13517</td>
<td>7.4 M</td>
<td>263</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:23:32.789</td>
<td>0.001 UDP</td>
<td>255.33.98.231:9875</td>
<td>128.122.1.249:9875</td>
<td>A...</td>
<td>0</td>
<td>2</td>
<td>938</td>
<td>2000</td>
<td>7.2 M</td>
<td>469</td>
<td>2</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:21:18.009</td>
<td>0.001 UDP</td>
<td>192.160.218.158:9616</td>
<td>242.190.27.953</td>
<td>0</td>
<td>2</td>
<td>12</td>
<td>924</td>
<td>12000</td>
<td>7.0 M</td>
<td>77</td>
<td>2</td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:23:42.956</td>
<td>0.001 UDP</td>
<td>171.217.137.258:52936</td>
<td>252.152.192.248:9672</td>
<td>0</td>
<td>6</td>
<td>288</td>
<td>2000</td>
<td>6.8 M</td>
<td>444</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:23:43.051</td>
<td>0.001 UDP</td>
<td>189.182.72.7:53</td>
<td>254.174.227.323780</td>
<td>0</td>
<td>4</td>
<td>828</td>
<td>4000</td>
<td>6.3 M</td>
<td>207</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:24:19.215</td>
<td>0.001 UDP</td>
<td>202.150.215.139:0</td>
<td>252.152.110.1031025</td>
<td>0</td>
<td>2</td>
<td>826</td>
<td>2000</td>
<td>6.3 M</td>
<td>413</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:24:19.214</td>
<td>0.001 UDP</td>
<td>202.150.215.139:0</td>
<td>252.152.110.621026</td>
<td>0</td>
<td>2</td>
<td>826</td>
<td>2000</td>
<td>6.3 M</td>
<td>413</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2006-04-21</td>
<td>03:24:19.214</td>
<td>0.001 UDP</td>
<td>202.150.215.139:0</td>
<td>252.152.110.621026</td>
<td>0</td>
<td>2</td>
<td>826</td>
<td>2000</td>
<td>6.3 M</td>
<td>413</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
Profiles:

- A profile is a specific view on the netflow data with nfdump filters applied.
- The profile applies to the graphical as well as to the numerical view.
- Profiles can be created from data in the past. (static)
- Profiles can be created from incoming data (continuous)
- Any views or processing options are available.
### nfdump and NfSen

![nfdump and NfSen](image)

#### Profile
- **Profile:** DNSttraf
  - Name of new profile. The naming follows the directory naming convention.
- **Description:** All port 53 traffic

#### Start
- **Format:** yyyy-mm-dd HH:MM
- **Start time of new profile:**
  - *Any time is accepted from 2006-04-02 01:15 (Start of the line profile) up to 2006-05-03 11:30. If left empty, the profile starts from now: 2006-05-03 11:30 (continuous profile).*

#### End
- **Format:** yyyy-mm-dd HH:MM
- **End time of new profile:**
  - *Must be later than start of the profile. Leave empty for a continuous profile.*

#### Sources
- **Downstream**
- **Upstream**
  - Peer1
  - Peer2

#### Filter
- **port 53 and ( tcp or udp )**

#### Max. Size
- **Maximum size, this profile may grow:** Any number is taken as MB, unless another scale is specified such as K, M, G, T or KB, MB, GB, TB. If set to 0, no size limit applies. Ex: 300, 300M, 2G etc.

#### Expire
- **Never**
  - *Expire time: This specifies the maximum lifetime for this profile. Data files older than this will be deleted. Any number is taken as hours unless another scale is specified such as d, day, days and/or h, hour, hours. If set to 0 or never, no time limit applies. Ex: 72, 72h, 4d 12h, 16days etc.*

---

2006 © SWITCH
Profile: ‘port 53 and (tcp or udp ):'
nfdump and NfSen

Example Profiles:

Filter: ‘( udp or tcp ) and port 53

Filter: ‘bytes < 100’

Filters may be as complex as the the filter syntax of nfdump allows.
Example: ‘((src net 172.16/16 and src port > 1024 ) or dst host 192.168.16.17 and dst port 80) and packets > 1000 and pps > 150’
**SoberR:** ‘tcp and dst port 587’

- **TCP**
- **UDP**
- **ICMP**
- **other**

**Profileinfo:**
- **Type:** history
- **Max:** unlimited
- **Exp:** never
- **Start:** Oct 01 2005 - 00:00
- **End:** Oct 07 2005 - 00:00

**Flow/s any protocol**
- Select [ ] left □ Mark
- Display: 1 day □ << < | ^ > >> >|
nfdump and NfSen

Incident analysis - profile a hacked host:
nfdump and NfSen

Plugins - what for?
• Monitoring and alerting.
• Track for known botnet masters and send notifications.
• Track for possible scanners or DoS attacks, not necessarily visible in the graph.
• Port Tracking.

Backend Plugins are:
• Simple Perl modules hooked into the NfSen backend.
• Automatically called at regular 5 Min intervals.

Frontend Plugins are:
• Simple PHP modules hooked into NfSen frontend.
• Called by selecting the tab.
nfdump and NfSen

NfSen Plugins:

Web Front-end
Frontend Plugins

Post Processing
Backend Plugins

Periodic Update
nfdump and NfSen

Backend Plugins:

```perl
# package CatchDos;
use strict;
# sub Init {
  # Init plugin
} # End of Init
sub run {
  my $profile = shift;
  my $timeslot = shift;
} # End of run
```

```bash
# @plugins = ( ['live', 'CatchDos'], 1;
```

**register**

```
backend Plugin
```

```
nfsen.conf
```

```
Runs automatically every 5 min
```

```
Report ...
```

```
output
```

```
@ Notification.pm
```

```
``
Cookbook for writing Backend Plugins:

• Select a plugin name: MyPlugin
• Create a Perl module named MyPlugin.pm
• Write your code.
• Try/debug your module offline using $BINDIR/testPlugin:
  
  ./testPlugin -p MyPlugin -P live -t 200603140800

• Store the file MyPlugin.pm in the directory $BACKEND_PLUGINDIR
  ( e.g. /data/nfsen/plugins )
• Register the plugin in nfsen.conf for the profiles in question:

```perl
@plugins = ( # profile    # modul
    # ['*', 'demoplugin'],
    [ 'live', 'MyPlugin'],
);```

```
#!/usr/bin/perl

package MyPlugin;

use strict;
# Periodic function
# input:  profilename
#        timeslot. Format yyyymmddHHMM e.g. 200503031200
sub run {
    my $profile  = shift;
    my $timeslot = shift;
    # Called at every cycle
    # Your code goes here

}

sub Init {
    # Do module init staff here

    # return 1 on success - module successfully loaded
    # return 0 on failure - module disabled
    return 1;
}

sub BEGIN {
    # Standard BEGIN Perl function - See Perl documentation
    # Called on loading the module

}

sub END {
    # Standard END Perl function - See Perl documentation
    # Called on unloading the module

}
nfdump and NfSen

Example Candidates for scanning activities:

```perl
# Define a nice filter:
# We like to see flows containing more than xxx packets
my $limit = 6000;
my $nf_filter = 'duration < 3500 and packets < 3 and bpp < 100 and src as 559';

# Periodic function
#   input: profilename
#          timeslot. Format yyyymmddHHMM e.g. 200503031200
sub run {
    my $profile = shift;
    my $timeslot = shift;
    syslog('debug', "CatchScanners run: Profile: $profile, Time: $timeslot");
    my %profileinfo = NfSen::ReadProfile($profile);
    my $netflow_sources = $profileinfo{'sourcelist'};
    # process all sources of this profile at once
    my @output = `nfdump -M PROFILEDATADIR/$profile/$netflow_sources -r nfcapd.$timeslot -a -A srcip,dstport -l $limit -f $nf_filter`;
    # Process the output and notify the duty team
}
```

(IP addresses anonymised)
nfdump and NfSen

Backend / Frontend Plugins:

Backend Plugin

```
package CatchDos;
use strict;

sub Init {
    # Init plugin
}

sub run {
    my $profile  = shift;
    my $timeslot = shift;
}
```

Nfsen.conf

```
#plugins = ( ['live', 'CatchDos'],
           1);
```

Frontend Plugin

```
/* Port Tracker
* Plugin */
function PortTracker_Run($plugi) {
    $portinfo = GetTopN($plugin_id,
                        $_SESSION["${plugin_id}…
                        ...
                    } // End of PortTracker_Run
```
Cookbook for writing Frontend Plugins:

• Write the Backend plugin: **MyPlugin**
• Create a PHP module named **MyPlugin.php**
• Write your code.
  – Must have 2 well defined functions:
    ```
    function <plugin_name>_ParseInput( $plugin_id )
    function <plugin_name>_Run( $plugin_id )
    ```
  – Have each a unique plugin ID: `$plugin_id`
  – Run at any time the user selects the plugin.
  – Profile read only information available in `$_SESSION['profileinfo']`
    example: `$_SESSION['profileinfo']['name']`
• Store the file `MyPlugin.php` in the directory `$_FRONTEND_PLUGININDIR`
  ( e.g. `/var/www/htdocs/nfsen/plugins` )
• Reload nfsen-run backgroud process: `$BINDIR/nfsen reload`
• Check correct load of module in syslog file.
nfdump and NfSen

<?

/*
 * MyPlugin plugin
*/

// Required functions
/*
 * This function is called prior to any output to the web browser and is intended
 * for the plugin to parse possible form data. This function is called only, if this
 * plugin is selected in the plugins tab
 */
function MyPlugin_ParseInput( $plugin_id ) {
    if ( isset($_POST["${plugin_id}_variable"])) { 
        } else { 
            $_SESSION[‘warning’] = “Warning …”;
            $_SESSION[‘error’] = “Error …”;
        }
    } // End of MyPlugin_ParseInput

/*
 * This function is called after the header with the navigation bar have been sent to the
 * browser. It’s now up to this function what to display.
 * This function is called only, if this plugin is selected in the plugins tab
 */
function MyPlugin_Run( $plugin_id ) {
    $_SESSION["${plugin_id}_variable"] = …
} // End of MyPlugin_Run

?>
Planned Plugin: Host behaviour based worm detection:
Result of a PhD network security research work in the context of the DDoSVax project at Swiss Federal Institute of Technology Zurich:
http://www.tik.ee.ethz.ch/~ddosvax/

Idea: Infected hosts show a different behaviour and can be put into different classes:

„Traffic“ class:
Worm infected hosts tend to send considerably more traffic than they receive.

„Responder“ class:
If many more hosts start to answer requests, they probably are victims of a worm.

„Connector“ class:
Worm infected hosts typically open many connections.
DDoS Vax: Host behaviour based worm detection:

Most interesting for worm detection are cardinalities of class combinations.
nfdump and NfSen

Figures @ SWITCH:
- Server: 2 x 3GHz 2GB Ram. Debian Linux Kernel 2.6.10
- 3TB (2TB + 1TB) AXUS Disk Raid
- XFS file system.
- Gigabit Ethernet interfaces.
- 5min workload avg. ca. 5%.
- 25GB Netflow data / day.
- About 41 days of netflow data available.
nfdump and NfSen

Next Steps - Todo list - a lot of work:
NfSen:
• more plugins ..
• Improved profiles.
• Improved interface.
• ...

nfdump:
• Related filters: ‘Malware Footprint Tracking’
  first { dst ip <A> dst port 445 bytes > 600 } 
  then { src ip <A> and dst ip 172.16.17.18 and dst port 80 } 
• Include more v9/sflow data in capture files.
• Realtime flow processing.
• Nesting directory levels for data organisation -> latest snapshot
• ...
nfdump and NfSen

Summary:

• Powerful and flexible tools for all sort of netflow tasks.
  – Network monitoring.
  – Incident Handling.
  – All sort of tracking …

• Open Source under BSD License.

• Cmd line tool: nfdump
  – Written in C. Runs on most *nix.
    Tested on Linux Kernel 2.4.* and 2.6.*, FreeBSD, OpenBSD, Solaris.
  – Available at http://nfdump.sourceforge.net

• Web based frontend: NfSen
  – Written in PHP and Perl.
  – Extendable using plugins.
  – Available at http://nfsen.sourceforge.net
nfdump and NfSen

Thank you for your attention. Any Questions?