Watch those Flows

12th TF-CSIRT Meeting
27. Mai 2004 Hamburg
Peter Haag haag@switch.ch
NFSEN (NetFlow Sensor) History

We got lots of email which made us thinking:

- “Watch your flows for …”
- “You’ve got bot if you see flow to … “
- “I’ve seen in our flows …”

Everybody was speaking about flows!

“So .. We need a tool!”

- to watch our flows.
- to find botnets.
- To analyse incident.
- To see trends.
- For reporting and alerting what we find.

In short: “Simply a tool which supports us in our daily work.”
NFSEN Usage - A tool to work with

With NFSEN you can:

• Display the network traffic situation.
• Easily navigate through the netflow data. (time based)
• Profile/monitor specific Networks/Hosts and events.
• Extensively filter the netflow data.
• Analyse the netflow data using the web based as well as the command line based interface.
• Create Top N statistics.
• Post process the netflow data for reporting and alerting.
NFSEN - Web Interface

Graphical View

Numerical View
### NFSEN - CLI output

```
cobolx nfdump -r /netflow0/nfSEN/spool/swiix1/nfcapd.200405170940 -S
Analysed flows 1969408
```

#### Top 10 flows packet count:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Address:Port</th>
<th>Dst IP Address:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 17 2004 09:27:24</td>
<td>904 TCP</td>
<td></td>
<td>49580 -&gt;</td>
<td>49649 -&gt;</td>
<td>435</td>
<td>348910</td>
<td>496.2 MB</td>
</tr>
<tr>
<td>May 17 2004 09:27:39</td>
<td>905 TCP</td>
<td></td>
<td>49582 -&gt;</td>
<td>49649 -&gt;</td>
<td>435</td>
<td>348030</td>
<td>492.2 MB</td>
</tr>
<tr>
<td>May 17 2004 09:29:16</td>
<td>840 TCP</td>
<td></td>
<td>49472 -&gt;</td>
<td>49477 -&gt;</td>
<td>435</td>
<td>345204</td>
<td>490.9 MB</td>
</tr>
<tr>
<td>May 17 2004 09:29:52</td>
<td>631 TCP</td>
<td></td>
<td>49493 -&gt;</td>
<td>49576 -&gt;</td>
<td>435</td>
<td>332951</td>
<td>473.6 MB</td>
</tr>
<tr>
<td>May 17 2004 09:32:20</td>
<td>746 TCP</td>
<td></td>
<td>49494 -&gt;</td>
<td>49493 -&gt;</td>
<td>119</td>
<td>286764</td>
<td>497.8 MB</td>
</tr>
<tr>
<td>May 17 2004 09:32:39</td>
<td>704 TCP</td>
<td></td>
<td>49576 -&gt;</td>
<td>49493 -&gt;</td>
<td>435</td>
<td>258203</td>
<td>362.7 MB</td>
</tr>
<tr>
<td>May 17 2004 09:37:18</td>
<td>403 TCP</td>
<td></td>
<td>20 -&gt;</td>
<td>59560 -&gt;</td>
<td>16352</td>
<td>224504</td>
<td>321.1 MB</td>
</tr>
<tr>
<td>May 17 2004 09:27:39</td>
<td>905 TCP</td>
<td></td>
<td>49580 -&gt;</td>
<td>59560 -&gt;</td>
<td>3418</td>
<td>207062</td>
<td>284.4 MB</td>
</tr>
</tbody>
</table>

#### Top 10 flows byte count:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Address:Port</th>
<th>Dst IP Address:Port</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 17 2004 09:27:24</td>
<td>904 TCP</td>
<td></td>
<td>49580 -&gt;</td>
<td>49649 -&gt;</td>
<td>435</td>
<td>348910</td>
<td>496.2 MB</td>
</tr>
<tr>
<td>May 17 2004 09:27:39</td>
<td>905 TCP</td>
<td></td>
<td>49582 -&gt;</td>
<td>49649 -&gt;</td>
<td>435</td>
<td>348030</td>
<td>492.2 MB</td>
</tr>
<tr>
<td>May 17 2004 09:29:16</td>
<td>840 TCP</td>
<td></td>
<td>49472 -&gt;</td>
<td>49477 -&gt;</td>
<td>435</td>
<td>345204</td>
<td>490.9 MB</td>
</tr>
<tr>
<td>May 17 2004 09:29:52</td>
<td>631 TCP</td>
<td></td>
<td>49493 -&gt;</td>
<td>49576 -&gt;</td>
<td>435</td>
<td>332951</td>
<td>473.6 MB</td>
</tr>
<tr>
<td>May 17 2004 09:32:20</td>
<td>746 TCP</td>
<td></td>
<td>49494 -&gt;</td>
<td>49493 -&gt;</td>
<td>119</td>
<td>286764</td>
<td>497.8 MB</td>
</tr>
<tr>
<td>May 17 2004 09:32:39</td>
<td>704 TCP</td>
<td></td>
<td>49576 -&gt;</td>
<td>49493 -&gt;</td>
<td>435</td>
<td>258203</td>
<td>362.7 MB</td>
</tr>
<tr>
<td>May 17 2004 09:37:18</td>
<td>403 TCP</td>
<td></td>
<td>20 -&gt;</td>
<td>59560 -&gt;</td>
<td>16352</td>
<td>224504</td>
<td>321.1 MB</td>
</tr>
<tr>
<td>May 17 2004 09:27:39</td>
<td>905 TCP</td>
<td></td>
<td>49580 -&gt;</td>
<td>59560 -&gt;</td>
<td>3418</td>
<td>207062</td>
<td>284.4 MB</td>
</tr>
</tbody>
</table>
Time slot: '200405170910' Profile: 'live'

TCP

UDP

ICMP

other

Mon May 17 09:10:00 2004 Packets/s any protocol

Min : 2.70 k Max : 32.82 k Avg : 12.00 k
Min : 15.25 k Max : 142.98 k Avg : 53.53 k
Min : 15.60 k Max : 123.19 k Avg : 52.24 k
Min : 24.88 k Max : 226.04 k Avg : 94.63 k

Mon May 17 09:10:00 2004
### 5Min Statistics accumulated values

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>swiba2</td>
<td>477980</td>
<td>4277442</td>
<td>3958123</td>
<td>197361</td>
<td>21895</td>
<td>100063</td>
<td>2.4 GB</td>
<td>2.3 GB</td>
<td>47.8 MB</td>
<td>1.2 MB</td>
</tr>
<tr>
<td>swice2</td>
<td>627523</td>
<td>14947267</td>
<td>14243784</td>
<td>401437</td>
<td>72630</td>
<td>294416</td>
<td>11.1 GB</td>
<td>10.8 GB</td>
<td>69.8 MB</td>
<td>5.5 MB</td>
</tr>
<tr>
<td>swice3</td>
<td>1665670</td>
<td>16430852</td>
<td>15220922</td>
<td>1042396</td>
<td>150325</td>
<td>17209</td>
<td>8.0 GB</td>
<td>7.8 GB</td>
<td>198.0 MB</td>
<td>13.6 MB</td>
</tr>
<tr>
<td>swix1</td>
<td>2339847</td>
<td>35864347</td>
<td>33736729</td>
<td>1522185</td>
<td>131736</td>
<td>473697</td>
<td>22.3 GB</td>
<td>21.7 GB</td>
<td>324.2 MB</td>
<td>14.6 MB</td>
</tr>
</tbody>
</table>

### Netflow Processing

**Source:** swix1

**Filter:**

- [ ] Show the first 10 flows
- [ ] Show aggregated netflows
- [ ] Show the first top 10 flows
- [ ] Show most seen flows
- [ ] Show most seen SRC IP addresses
- [ ] Show most seen DST IP addresses

**Analysed flows:** 1914267

**Time window:** May 17 2004 08:54:56 - May 17 2004 09:14:57

#### Top 10 flows packet count:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Address:Port</th>
<th>Dst IP Address:Port</th>
<th>Packets</th>
<th>Bytes Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 17 2004 08:59:06</td>
<td>906 TCP</td>
<td>49477</td>
<td>435</td>
<td>38211</td>
<td>543.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:35</td>
<td>910 TCP</td>
<td>49472</td>
<td>435</td>
<td>377184</td>
<td>536.7 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:53</td>
<td>783 TCP</td>
<td>80</td>
<td>1537</td>
<td>207530</td>
<td>228.3 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:46</td>
<td>1116 TCP</td>
<td>49373</td>
<td>119</td>
<td>204894</td>
<td>290.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 09:13:45</td>
<td>47 TCP</td>
<td>20</td>
<td>18399</td>
<td>189153</td>
<td>267.2 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:58</td>
<td>979 TCP</td>
<td>35264</td>
<td>119</td>
<td>181183</td>
<td>256.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:59</td>
<td>901 TCP</td>
<td>49444</td>
<td>119</td>
<td>165984</td>
<td>235.6 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:58</td>
<td>901 TCP</td>
<td>35275</td>
<td>119</td>
<td>164992</td>
<td>233.9 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:46</td>
<td>905 TCP</td>
<td>49378</td>
<td>119</td>
<td>164904</td>
<td>234.0 MB</td>
<td></td>
</tr>
</tbody>
</table>

#### Top 10 flows byte count:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Address:Port</th>
<th>Dst IP Address:Port</th>
<th>Packets</th>
<th>Bytes Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 17 2004 08:59:06</td>
<td>906 TCP</td>
<td>49477</td>
<td>435</td>
<td>38211</td>
<td>543.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:35</td>
<td>910 TCP</td>
<td>49472</td>
<td>435</td>
<td>377184</td>
<td>536.7 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:53</td>
<td>783 TCP</td>
<td>80</td>
<td>1537</td>
<td>207530</td>
<td>228.3 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:46</td>
<td>1116 TCP</td>
<td>49373</td>
<td>119</td>
<td>204894</td>
<td>290.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 09:13:45</td>
<td>47 TCP</td>
<td>20</td>
<td>18399</td>
<td>189153</td>
<td>267.2 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:58</td>
<td>979 TCP</td>
<td>35264</td>
<td>119</td>
<td>181183</td>
<td>256.8 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:59</td>
<td>901 TCP</td>
<td>49444</td>
<td>119</td>
<td>165984</td>
<td>235.6 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:55:58</td>
<td>901 TCP</td>
<td>35275</td>
<td>119</td>
<td>164992</td>
<td>233.9 MB</td>
<td></td>
</tr>
<tr>
<td>May 17 2004 08:56:46</td>
<td>905 TCP</td>
<td>49378</td>
<td>119</td>
<td>164904</td>
<td>234.0 MB</td>
<td></td>
</tr>
</tbody>
</table>
Profiles:

- A profile is a specific view on the netflow data with input 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)

Web Interface:
Switch to profile 'Witty'

Mon Mar 22 12:00:00 2004 Flows/s any protocol

- swiba2: Min: 0.00, Max: 245.33, Avg: 34.43
- swice2: Min: 2.22, Max: 1.27, Avg: 149.11
- swice3: Min: 54.44, Max: 1.29, Avg: 165.37
- Swi1x1: Min: 80.00, Max: 255.42, Avg: 42.07
NFSEN - overview

Various input data:
- Malicious IP’s
- Worm characteristics
- Hosts/Nets to monitor

154.3.2.2
123.3.5.78
4.89.5.132
89.4.3.54
...

Summary:
monitored:
...

Alerting

From: cert@switch.ch
To: security@
Subject: most likely compromised system
Dear Security Team,
.....
please check & act accordingly to your own policy
...

NFSEN Tools

“nfdump” tools are used for NFSEN:

• Comparable to tcpdump but for netflow data.
• Efficient filter engine: > 4 Mio flows/s on 3GHz Intel.
• Statistics:
  Top N flows for packets and bytes
  Top N src and/or dst IP addresses
• Powerful pcap like filter syntax.
  ‘( tcp and dst net 172.16/16 and dst port > 1024 ) or ( …’
Figures:
- Server: 2 x 3GHz Intel 2GB Ram. Linux Debian 2.4.25
- 3TB (2TB + 1TB) disk space XFS file system.
- GB Ethernet interfaces.
- Workload 5min avg. < 5%.
- 300 MB Netflow data / 5 min.
- About 35 days of netflow data available.
Success Stories:

• **Analysing incidents: Profiles are your friends**
  – Find all network connections of a hacked host.
  – Find botnet command masters.
    » Find other hosts connected to this botnet command master.
  – Find FTP main masters.
  – Find other hosts being infected by hacked host.

• **Observe worm propagation: online profiles**

• **Alerting worm infections:**
  – Watch for known network patterns and inform customers about their infected hosts.
Next steps:
• Improving Web Interface.
• Improve Profiling.
• Better Alerting.
• Combine time slices for analysing.
• nfdump tools become a sourceforge project.
Questions?

Send me an email: haag@switch.ch