NERD: Network Emergency Responder & Detector

Wim.Biemolt@surfnet.nl

2nd FloCon, Pittsburgh, September, 2005.
SURFnet5 network

- Operational
  - Since September 2001
- Cisco 12416 routers
- Backbone: 10Gbps
- Connections: 1Gbps
- Dual stack (6PE)
- Incident detection
  - SURFnet & TNO: 2002
- Decommissioning
  - End of December 2005
Incident response tools

- SURFstat
  - mrtg/rrdtool
- Research
  - syslog
  - Netflow
    - promising at the required speeds (>10 Gbps)
    - sampled (ip flow-sampling-mode packet-interval 100)
      - Full data analysis requires high-end equipment
- Prototype
  - cflowd (caida)
    - no longer supported
  - gnuplot, mysql, php
  - Not open-source
Prototype

Network Emergency Responder & Detector

Show all alarms from 0 days ago, up to 0 days ago. Show

The alarms between 2005-09-11 and 2005-09-12

The query took approximately 0.019 seconds.

<table>
<thead>
<tr>
<th>Destination IP address</th>
<th>Hostname</th>
<th>Flows per 5 minutes</th>
<th>Average packets per flow</th>
<th>Average bytes per flow</th>
<th>Average destination port</th>
<th>Starttime</th>
<th>Stoptime</th>
<th>Continuing</th>
</tr>
</thead>
<tbody>
<tr>
<td>140.165.67.68</td>
<td><a href="mailto:info@surf-europe.com">info@surf-europe.com</a></td>
<td>6542</td>
<td>1</td>
<td>157</td>
<td>47467</td>
<td>2005-09-11 14:15:07</td>
<td>2005-09-11 14:39:08</td>
<td>1</td>
</tr>
<tr>
<td>131.113.10.67</td>
<td><a href="mailto:spammer@surf-europe.com">spammer@surf-europe.com</a></td>
<td>29700</td>
<td>1</td>
<td>74</td>
<td>39930</td>
<td>2005-09-11 14:33:05</td>
<td>2005-09-11 14:39:06</td>
<td>1</td>
</tr>
<tr>
<td>216.10.20.39</td>
<td>-</td>
<td>5555</td>
<td>1</td>
<td>142</td>
<td>47329</td>
<td>2005-09-11 14:39:06</td>
<td>2005-09-11 14:39:06</td>
<td>1</td>
</tr>
<tr>
<td>194.10.20.39</td>
<td><a href="mailto:info@surf-europe.co.uk">info@surf-europe.co.uk</a></td>
<td>15955</td>
<td>1</td>
<td>157</td>
<td>47286</td>
<td>2005-09-11 11:03:03</td>
<td>2005-09-11 11:27:03</td>
<td>0</td>
</tr>
<tr>
<td>216.10.20.39</td>
<td>-</td>
<td>4012</td>
<td>1</td>
<td>149</td>
<td>47560</td>
<td>2005-09-11 09:45:06</td>
<td>2005-09-11 09:45:06</td>
<td>0</td>
</tr>
</tbody>
</table>
Alarm

131.65.82.107
ac.jp

Perform:
Whois
Traceroute
Nmap

PS. Nmap is a portscanner, not everybody appreciates being portscanned. Use at your own risk.

Click on the following filenames to see detailed information:
flows.20050911 14:42:52+0200
flows.20050911 14:37:49+0200
flows.20050911 14:32:46+0200

Switch to this IP address:

Go
High-quality Internet for higher education and research
Hardware

- Dell PowerEdge 1650
  - 04-2002, RedHat 7
  - 1x 1.4GHz, 1GB, 3x 36GB
- Dell PowerEdge 2650
  - 12-2003, FreeBSD 4.11
  - 2x 3GHz, 4GB, 5x 146GB
- Dell PowerEdge 2850
  - 10-2004, FreeBSD 5.4
  - 2x 3.4GHz, 6GB, 6x 146GB
- Dell PowerEdge 2850
  - 06-2005, FreeBSD 6.0
  - 2x 3.6GHz, 4GB, 6x 300GB
- SunFire V240
  - 12-2004, Solaris 10
  - 2x 1.5GHz, 4GB, 4x 146GB

http://www.switch.ch/tf-tant/floma/sw/samplicator/
Some specs of the new NERD

- nerdd, analysis
  - boost libraries, MySQL database, php, plplot
- Netflow versions
  - V5 (tested)
  - V9 (IPFIX)
- Platforms tested
  - FreeBSD
  - Linux
- Apache Open Source Licence v2.0
Software Architecture

- Collector
  - Simple UDP receiver
- Pre-processor
  - Source specific functions
- Data kept in memory
  - Real-time analysis
- Data stored on disk
  - Post analysis
Real-time and post analysis

• Real time analysis
  – Rules can be used for ‘real-time’ analysis
    • A rule is a combination of filters, clusters and a threshold for some metric (e.g. number of flows)
  – Example of a rule
    • Filter “port=445”, cluster “dst IP”, threshold=1000 flows/min
  – Results in an alarm if a host receives more then 1000 flows/min on TCP port 445
  – Output formatting: alarm in database
  – Every x minutes the rules (1…n) are executed

• Post analysis
  – Executed at user request
  – Rules without threshold
  – Output formatting: flow-tools like text file, graphical output
Functionality – Filters & Clusters

- Sample of Netflow data

<table>
<thead>
<tr>
<th>src</th>
<th>prt</th>
<th>dst</th>
<th>prt</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>2000</td>
<td>10.0.0.2</td>
<td>23</td>
</tr>
<tr>
<td>10.0.0.3</td>
<td>1000</td>
<td>10.0.0.2</td>
<td>22</td>
</tr>
<tr>
<td>10.0.0.6</td>
<td>2000</td>
<td>10.0.0.2</td>
<td>22</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>1000</td>
<td>10.0.0.3</td>
<td>23</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>1000</td>
<td>10.0.0.3</td>
<td>23</td>
</tr>
</tbody>
</table>

- Example: filter “src port=2000”

<table>
<thead>
<tr>
<th>src</th>
<th>prt</th>
<th>dst</th>
<th>prt</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>2000</td>
<td>10.0.0.2</td>
<td>23</td>
</tr>
<tr>
<td>10.0.0.6</td>
<td>2000</td>
<td>10.0.0.2</td>
<td>22</td>
</tr>
</tbody>
</table>

- Example: filter, cluster “dst port” & count flows

<table>
<thead>
<tr>
<th>prt</th>
<th># of flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
</tr>
</tbody>
</table>
Real-time analysis - configuration

NERD
Network Emergency Responder & Detector

Rules for real-time analysis

Source: neredd memory
timeIntervalSec 1200
sleepTimeSec 200

Rule 1
Filter
- src,dst_add
- dst_port
- src_port
Add Expression
- ×

Rule 2
Filter
- src,dst_add
- dst_port
- src_port
Add Expression
- ×

Cluster 1
- Det
- Add rule
- src,dst_add
- dst_port
- src_port
Count: Bins
Threshold: 1000
Add new cluster

Cluster 2
- Det
- Add rule
- src,dst_add
- dst_port
- src_port
Count: Bins
Threshold: 1000
Add new cluster

High-quality Internet for higher education and research
### Alarms

**NERD**

**Network Emergency Responder & Detector**

<table>
<thead>
<tr>
<th>Starttime</th>
<th>Stoptime</th>
<th>Rulename</th>
<th>Alarm message (key, keyval, counterval)</th>
<th>Limit</th>
<th>Cont.</th>
<th>Analyse</th>
</tr>
</thead>
<tbody>
<tr>
<td>06-Sep-2005 08:14:15</td>
<td>06-Sep-2005 12:13:17</td>
<td>rule5</td>
<td>ipv4_dst_addr 2001</td>
<td>1</td>
<td>Yes</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 11:35:10</td>
<td>06-Sep-2005 12:04:50</td>
<td>rule5</td>
<td>ipv4_dst_addr 2002</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 12:26:26</td>
<td>06-Sep-2005 12:34:50</td>
<td>rule5</td>
<td>ipv4_dst_addr fe80</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 12:31:28</td>
<td>06-Sep-2005 12:04:52</td>
<td>rule5</td>
<td>ipv4_dst_addr 2001</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 12:38:52</td>
<td>06-Sep-2005 12:48:02</td>
<td>rule4</td>
<td>ipv4_dst_addr 130</td>
<td>98 flows.</td>
<td>800</td>
<td>No</td>
</tr>
<tr>
<td>06-Sep-2005 12:30:52</td>
<td>06-Sep-2005 12:48:02</td>
<td>rule4</td>
<td>ipv4_dst_addr 143</td>
<td>939 flows.</td>
<td>800</td>
<td>No</td>
</tr>
<tr>
<td>06-Sep-2005 12:43:02</td>
<td>06-Sep-2005 12:48:02</td>
<td>rule5</td>
<td>ipv4_dst_addr 2001</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 12:43:13</td>
<td>06-Sep-2005 12:48:02</td>
<td>rule5</td>
<td>ipv4_dst_addr fe80</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 11:48:23</td>
<td>06-Sep-2005 12:14:22</td>
<td>rule4</td>
<td>ipv4_dst_addr 130</td>
<td>93 flows.</td>
<td>800</td>
<td>No</td>
</tr>
<tr>
<td>06-Sep-2005 11:52:33</td>
<td>06-Sep-2005 12:14:22</td>
<td>rule5</td>
<td>ipv4_dst_addr 2001</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
<tr>
<td>06-Sep-2005 12:00:58</td>
<td>06-Sep-2005 12:14:22</td>
<td>rule5</td>
<td>ipv4_dst_addr fe80</td>
<td>1</td>
<td>No</td>
<td>Analyse</td>
</tr>
</tbody>
</table>

**Search**

**Delete alarms older than**

---

**High-quality Internet for higher education and research**
Analysis – IPv4
Analysis – IPv6

```plaintext
# --- ---- ---- Report Information --- ---- ----
# build-version: 1
# Cluster name: cluster0
#
# Description:
# Threshold: 0
# timeFirst: 2005-09-06 08:14:05
# timeLast: 2005-09-06 13:13:18
# recn: ipv6_src_addr,flows

2001:610:510:0:: = 5
2001:610:508:0:: = 2
```
Current Research and Development

• Geant2 JRA2
  – NERD is one of the monitoring toolsets
• LOBSTER project
  – Integration
• Student
  – Analysis and visualisation of worm behaviour
• Ph.D. from Vrije Universiteit (VU)
  – Interaction of Netflow and Full Packet inspection
• From application to framework
  – Other data sources, combining different data
  – Other data output
Questions

- More information and download of NERD
  - www.nerdd.org