Who doesn’t like these conferences!? my wife…
Agenda

- Snort and Sourcefire
- What we should know about SCADA
- SCADA model for our demo
- Live presentation
- Two words about the NextGen IPS
About Sourcefire

- Founded in 2001 by Snort Creator, Martin Roesch, CTO
- Polska: Krzysztof Rocki, Michał Ceklarz
- FY2010 Revenue: $130.6M
- 12 offices worldwide, 380 employees
- Over 4000 commercial/enterprise/government customers
- #1 in IPS Detection by NSS Labs (96.7% default)
- Recognized by Forbes as Fastest-Growing company in Security (2011)
- NASDAQ: FIRE
SCADA

- **Supervisory Control And Data Acquisition**
  - Evolved from analog signaling from the past into TCP/IP based signaling:
    - Human maintained
    - Leased telephone line
    - Circuit switched lines
    - Packet Switched lines
SCADA’s connectivity

- **Modbus TCP**

  - **Function code** – reading/writing coils/registers
  - **Address** - offset into register list
  - **Length** - number of bits and coils
  - **Data** – what you want to put to the device
  - **UnitID** – which unit under the same IP address
SCADA

- Functions and elements
  - Data Acquisition:
    - sensors (digital ‘on’ and ‘off’ or analog ‘how much?’)
    - relays
  - Data Communication:
    - Comm. Networks
  - Data Presentation:
    - Remote Terminal Unit – RTU
    - Historian used for storage
  - Control:
    - Programmable Logic Controller – PLC
    - Human-Machine Interface – HMI
    - Supervisory Computer System - SCS
SCADA model

Data Control  Data Presentation  Data Comm.  Data Acquisition

PLC/HMI/SCS  RTU/Historian  Cables/Radio  Sensors/Relays
Our SCADA model

Sourcefire IPS & Attacker

Alarm

Interlocks

Cooling System

Dehumidifier

RTU & PLC
Demonstration Time!
Real world example
Open Source Snort

- Global IDS/IPS standard
- Largest community contributing to attack detection rules
- Easy to integrate
- Ran in parallel with Sourcefire
- Global Portal www.snort.org
Next-Gen IPS – The Power of Awareness

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Behavior</th>
<th>Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know what’s there, what’s vulnerable, and what’s under attack</td>
<td>Identify change and enforce policy on hundreds of applications</td>
<td>Detect anomalies in configuration, connections and data flow</td>
<td>Know who is doing what, with what, and where</td>
</tr>
</tbody>
</table>

- **Network**
- **Application**
- **Behavior**
- **Identity**
Next-Generation IPS

Defense Center

Intrusion Prevention

Awareness technologies

Networks, Apps, Behavior, Users

SSL Inspection

Virtualisation

vmware, Xen
As part of this test, Sourcefire submitted the **3D8260 IPS Appliance**

**NSS Labs’ Rating: Recommend**

<table>
<thead>
<tr>
<th>Product</th>
<th>Effectiveness</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcefire 3D8260</td>
<td>97.6%</td>
<td>27,600 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Total Number of Exploits Run</th>
<th>Total Number Blocked</th>
<th>Block Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Configuration</td>
<td>1,179</td>
<td>1138</td>
<td>96.5%</td>
</tr>
<tr>
<td>Tuned Configuration</td>
<td>1,179</td>
<td>1151</td>
<td>97.6%</td>
</tr>
</tbody>
</table>
www.linkedin.com

Chrumkarnia – Snort PL