NETWORK FLOW ANALYSIS

Blackhat USA 2008
Bruce Potter

gdead@shmoo.com
bpotter@pontetec.com
INTRODUCTIONS

- **Bruce Potter**
  - Founder of Ponte Technologies
    - Focus on advanced defensive technologies
  - Founder of The Shmoo Group
    - We run ShmooCon as well as other events
  - Co-author of several books and other stuff
    - *802.11 Security*
    - *Mastering FreeBSD and OpenBSD Security*
    - *Mac OS X Security*

- Don’t believe anything you hear in Vegas
  - It’s mostly made up for publicity, either personal or corporate
  - We’re not formally trained… we shoot from the hip
FIRST, A PLUG

- No, I don’t get paid for this
- We’ll be talking a lot about data representation and visualization
- This is not something to be entered into lightly… there’s a lot of science and theory behind data visualization
  - Unfortunately it’s hard to bring analysis and visualization concepts to the lay person in a reasonable amount of time
EDWARD TUFTE

- Probably best know for his slagging on PPT
  - Created the Gettysburg Address as a PPT… amusing
- Published a series of books on data representation and visualization
  - *Visual Explanations*
  - *Envisioning Information*
  - *The Visual Display of Quantitative Information*
  - *Beautiful Evidence*
- Teaches 1 day classes around the country on data representation and visualization.
  - Again, I’m not paid for any of this, but I seriously recommend you go if you can
  - It’s darn near a religious experience for some
LET’S HAVE SOME STRUCTURE TO OUR DISCUSSION

Academic / Engineering

IT Security Operations

Software

Network

IT Operations

Honeypots

IDS, IR & Flow Analysis

Software Security & Software ACL’s

Firewalls & AAA Services

Patch management, procedures, policy

Sophistication and Operational Cost
WHAT IS NETWORK ANALYSIS?

- Quite simply, looking at evidence on or from the network in order to determine information regarding any of the following:
  - Security
  - Availability
  - Performance
  - Capability
  - Integrity
  - … really, any of the “ilities” (yes, performance is an “ility” 😊)
MEANS FOR EXECUTING NETWORK ANALYSIS

- Basically, analysis involves
  - Collecting and storing data
  - Distilling and stirring the data around
  - Analyzing the results

- Lots of ways to get evidence from the network
  - SNMP data from routers and switches
  - Raw packet captures
  - Auditing information from existing network infrastructure (IDS, Firewalls, VPN gateways)
  - Network Flows

- Each has various advantages and disadvantages
  - Many existing products
  - However, doing “analysis” with these products takes work… and do you really have time to do analysis or should you be configuring your firewall and fighting other fires in your network?
**A VIEW OF CURRENT THREAT SPACE**

<table>
<thead>
<tr>
<th>Highly Targeted</th>
<th>Skilled, Motivated</th>
<th>General Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Threat</td>
<td>Org Crime, Nation State</td>
<td>Worms, virus,</td>
</tr>
</tbody>
</table>

**Written Off**
Or at least basically ignored. Very difficult with today’s technology.

**“Solved” Problem**
AV, AS, IDS, Firewalls. These tools are highly automated and geared towards compliance.
A VIEW OF CURRENT THREAT SPACE

Highly Targeted
Insider Threat

Skilled, Motivated
Org Crime, Nation State

General Purpose
Worms, virus, "Solved" Problem

Written Off
Or at least basically ignored. Very difficult with today’s technology.

???
Requires some manual work as well as a different set of tools than is currently available.

“Solved” Problem
AV, AS, IDS, Firewalls.
These tools are highly automated and geared towards compliance.

Need to make analysts more effective
Collect, distill, and analyze the data. Not complicated, and lots of prior art. However for the public security product space, it might as well be rocket science.
TYPES OF SECURITY ANALYSIS TO BE PERFORMED - DEPTH FIRST VS. BREADTH FIRST

- Depth first
  - Depth first security analysis is what forensic analysts usually do
  - This type of analysis makes sense when you already know what you’re looking for or where you’re going to find it
  - Unfortunately it’s also the type of analysis that many ad hoc security analysts end up doing
    - Tools like grep and normal shell scripting foo lead to this type of analysis

- Breadth first
  - Much more useful when you don’t know what you’re looking for or where to look
    - The reality for most enterprises
  - Requires more specialized tools to help distill the data first
WHAT DO THESE GRAPHS HAVE IN COMMON?
TYPES OF SECURITY ANALYSIS – TIME DOMAIN VS. FREQUENCY DOMAIN

- Time Domain analysis is common with most “enterprise management” tools.
  - Most operators care about what’s going on minute to minute and how that compares what happened a minute/hour/day/week ago.
  - OSS tools like MRTG have made a lot of ppl very happy over the years.
  - Unfortunately tools like MRTG have created blinders on most operators who end up believing time series analysis is THE ONLY analysis.
LIMITATIONS OF TIME DOMAIN ANALYSIS

- There are others aspects of the data that get lost in the process of rolling everything together to make a pretty graph that varies over time
  - Per host, who is sending the most data outbound? Who is pulling in the most data?
  - Per host, who is talking to the most DSL hosts? The most Asia-Pacific hosts?
  - How many hosts are speaking more than 3 protocols? 4? 5? 100?

- Time domain analysis won’t tell you any of these answers
  - MRTG and the other tools are NOT geared up towards this.
WHAT IS THIS GRAPH?

Could be anything… Size of emails? Traffic sent per host? Number of hosts spoken to per host? Documents printed per day?
WHAT IS THIS GRAPH?

Could be anything…. Size of emails? Traffic sent per host? Number of hosts spoken to per host? Documents printed per day?

Probably OK data…
WHAT IS THIS GRAPH?

Might not be “OK” data…

Need to have a closer look.

Could be anything…. Size of emails? Traffic sent per host? Number of hosts spoken to per host? Documents printed per day?
WHAT IS A FLOW?

- Data regarding a unidirectional flow of information through a network
  - Nothing more complicated than that
REASONS TO CARE ABOUT NETWORK FLOWS

- Great visibility into a network without a ton of processor power required on the collection and analysis hosts
  - More detail than SNMP
  - Less complicated than full packet dumps
- Relatively cheap for the routers to export
- Your network infrastructure is already inline and sees all your data
- Netflow records take up little bandwidth
- Advanced statistical analysis can uncover policy violations, botnets, malware, etc.
Frequency Domain Analysis

- Looking at how often an event occurred per a given metric (per host, per subnet, per protocol, etc) rather than *when* an event occurred in relation to other events
  - Not a complicated concept
  - However, it is a concept geared more toward *analysts* rather than *operators*.
  - Few tools available today are focused on analyzing data; rather the tools are designed to fix a current problem and move on.
OTHER TYPES OF ANALYSIS

- Things can get really complicated beyond these basics
  - Correlation within a dataset – “how often was traffic with >2 ratio of outbound traffic going to Asia on weekends”
  - Correlation across multiple datasets – “How often is a small HTTP outbound connection followed by a login from the domain controller”
- These types of analysis get computationally expensive
  - But certainly not impossible. Q1Labs Qradar product does a good job of correlating data as it’s coming in. NetWitness does an amazing job at it, but it’s really a huge product to bring in house.
WHAT IS A FLOW?

- Data regarding a unidirectional flow of information through a network
  - Nothing more complicated than that
Flow1: src:A:36812, dst: B:80,
EXAMPLE

Flow1: src:A:36812, dst: B:80
Flow2: src:B:80, dst:A:36812
EXAMPLE

Flow1: src:A:36812, dst: B:80 (updated)
Flow2: src:B:80, dst:A:36812 (updated)
Flow1: src:A:36812, dst: B:80 (final)
Flow2: src:B:80, dst:A:36812 (final)
NOTE: The analysis capability may be on another host.
WHEN IS A FLOW RECORD GENERATED?

- Four different situations cause a flow record to be generated (general rules of thumb here, NOT set in stone!)
  - A flow terminates normally
    - I.e: a TCP session has a packet with the FIN bit set
    - Only works for session based protocols
  - The monitoring device does not see a packet in MAXIDLE time
    - Basically, if some period of time goes by (think 1-2 minutes) where no packets are seen, the router will free up memory by flushing the flow and presuming it dead
    - This is usually a tunable option. Low values may give false positives but keep the memory footprint small. High values give better data but can make for HUGE mem requirements
WHEN IS A FLOW RECORD GENERATED?

- Full Cache – The router is getting pushed too hard
- The monitoring device sees active data for more than MAXACTIVE time
  - There are times when a session might run for a LONG time.
  - Rather than get one flow record for it at the very end that throws everything off, a flow will be expired.
  - This does NOT mean a router closes the session… just the accounting information gets flushed
  - Again, this is usually tunable. Think 5-30 minutes
  - It should be noted that because of these types of issues, netflow data does not make good realtime bandwidth monitoring feeds.
    - Huge FTP downloads, with a 30 min MAXACTIVE timer will show huge spikes in bandwidth use, sometimes dramatically exceeding the maximum available real bandwidth
    - Use SNMP traffic data instead… much more accurate
DOING REAL TIME TRAFFIC ANALYSIS

- If you do want to use NetFlow to monitor bandwidth, then you’ll have to futz with the timers
  - Terminating flow accounting on a flow that’s reached MAXACTIVE does not mean the flow is done
  - Your collector should be able to put the pieces back together
    - Either based on heuristics or on TCP flags (if it’s TCP based)
  - Example – Set the active timer on your router to 1 minute
    - Certainly, this prematurely terminate the accounting record and generate multiple flows
    - Your collector may have MAXACTIVE set to 6 hours. Many few flows will be terminated incorrectly and most flows will be reconstructed by the collection engine
    - This gives you 1 minute resolution on traffic
  - Not good enough? Do port monitoring on your switches and graph that 😊
**HARDWARE IMPLICATIONS**

- Check the router to see what it’s got left in the CPU and memory buckets

```bash
rtr#show proc cpu
CPU utilization for five seconds: 37%/35%; one minute: 42%; five minutes: 41%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 8180 2013277 4 0.00% 0.00% 0.00% 0 Load Meter
2 14255652 130927068 108 0.00% 0.05% 0.06% 0 OSPF Hello
3 88398944 874468 101089 0.00% 0.58% 0.68% 0 Check heaps
4 221640 408951 541 0.00% 0.00% 0.00% 0 Pool Manager
5 0 2 0 0.00% 0.00% 0.00% 0 Timers
6 32457048 72469861 447 0.00% 0.00% 0.00% 0 ARP Input
Etc...
router>show processes memory
Total: 106206400, Used: 7479116, Free: 98727284
PID TTY Allocated Freed Holding GetbufsRetbufs Process
0 0 81648 1808 6577644 0 0 *Init*
0 0 572 123196 572 0 0 *Sched*
0 0 10750692 3442000 5812 2813524 0 *Dead*
1 0 276 276 3804 0 0 Load Meter
2 0 228 0 7032 0 0 CEF Scanner
3 0 0 0 6804 0 0 Check heaps
Etc...
```
BUILDING YOUR OWN?

- You’ll need a box or two…
  - You want reliable boxes. It should be noted that these boxes will be inline with your network. So they should be as reliable as an ethernet cable.
  - Needs to be able to handle the flow generation software without much hassle.
    - Not really too hard. You can easily push wirespeed 100Mb/s on a 1GHz processor with an Linux distro.
    - Need a fair bit of memory (1GB should do fine, might get away with 512MB).
    - Disk is not an issue because the sensor won’t be storing the data.
  - Buy fail open (fail closed?) Ethernet cards that will turn into a cable upon crash or power failure.
    - Not cheap… like $200-$500 each.
SOFTFLOWD

- There are a variety of NetFlow sensors available in the OSS world
  - I’m partial to Softflowd
    - Stable, good licence
    - Easy to configure
    - http://www.mindrot.org/projects/softflowd/
  - Runs quickly and easily on Linux and FreeBSD (w00t! Go FreeBSD!)
- The basic idea is that you create a bridge group of two ethernet interfaces
  - This is allows you to drop a softflow box inline without modifying any of your IP/subnet architecture
- Then bind softflowd to the bridge group and tell it where to export the flows
  - That’s it…
# Assume that fe 0/1 is the inbound from the Internet and fe0/2 is the LAN facing interface
router(config)#interface FastEthernet 0/1
router(config-if)#ip route-cache flow
router(config-if)#exit
#since by default this is only for inbound, repeat for the other interface
router(config)#interface FastEthernet 0/2
router(config-if)#ip route-cache flow
router(config-if)#exit
# configure the netflow collector IP and port
router(config)#ip flow-export destination
  192.168.90.10 9996
# by default, the flows will be sourced from
  lo0. change if needed
router(config)#ip flow-export source
  FastEthernet 0/1
router(config)#ip flow-export version 5
# super aggressive timeout for active to keep
data flowing into the collector (mins)
router(config)#ip flow-cache timeout active 1
# also aggressive (seconds)
router(config)#ip flow-cache timeout inactive 15
show ip cache flow

IP packet size distribution (489639251 total packets):

1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
0.000 0.992 0.000 0.003 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
0.000 0.000 0.000 0.003 0.000 0.000 0.000 0.000 0.000 0.000 0.000
**CHECKING UP**

IP Flow Switching Cache, 8913408 bytes
- 5088 active, 125984 inactive, 1843766371 added
- 805412120 ager polls, 0 flow alloc failures
- Active flows timeout in 30 minutes
- Inactive flows timeout in 15 seconds
- Last clearing of statistics never

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Packets /Sec</th>
<th>Bytes /Sec</th>
<th>Packets Active /Sec</th>
<th>Idle Flows /Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-Telnet</td>
<td>28084</td>
<td>0.0</td>
<td>1</td>
<td>45</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-FTP</td>
<td>172835</td>
<td>0.0</td>
<td>1</td>
<td>47</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-FTPD</td>
<td>2818</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-WWW</td>
<td>5551226</td>
<td>1.2</td>
<td>1</td>
<td>53</td>
<td>1.3</td>
</tr>
<tr>
<td>TCP-SMTP</td>
<td>4179</td>
<td>0.0</td>
<td>1</td>
<td>42</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-X</td>
<td>2594</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-BGP</td>
<td>2546</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-NNTP</td>
<td>2554</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-Frag</td>
<td>177</td>
<td>0.0</td>
<td>2</td>
<td>269</td>
<td>0.0</td>
</tr>
<tr>
<td>TCP-other</td>
<td>528636</td>
<td>0.1</td>
<td>1</td>
<td>40</td>
<td>65.5</td>
</tr>
<tr>
<td>UDP-DNS</td>
<td>11596</td>
<td>0.0</td>
<td>1</td>
<td>54</td>
<td>0.0</td>
</tr>
<tr>
<td>UDP-NTP</td>
<td>723</td>
<td>0.0</td>
<td>2</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>UDP-TFTP</td>
<td>763</td>
<td>0.0</td>
<td>3</td>
<td>37</td>
<td>0.0</td>
</tr>
<tr>
<td>UDP-Frag</td>
<td>25</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
</tr>
<tr>
<td>UDP-other</td>
<td>169720402</td>
<td>39.5</td>
<td>1</td>
<td>40</td>
<td>46.2</td>
</tr>
<tr>
<td>ICMP</td>
<td>275131</td>
<td>0.0</td>
<td>10</td>
<td>759</td>
<td>0.6</td>
</tr>
<tr>
<td>IGMP</td>
<td>36</td>
<td>0.0</td>
<td>1789</td>
<td>1246</td>
<td>0.0</td>
</tr>
<tr>
<td>IP-other</td>
<td>7</td>
<td>0.0</td>
<td>19</td>
<td>64</td>
<td>0.0</td>
</tr>
<tr>
<td>Total:</td>
<td>176304332</td>
<td>41.0</td>
<td>2</td>
<td>44</td>
<td>113.9</td>
</tr>
</tbody>
</table>

---

Copyright 2008 - Bruce Potter
<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcPDstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hs9/1/0</td>
<td>192.168.2.51</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>04A9</td>
<td>614K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.47.72</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>05F9</td>
<td>281K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.49.52</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>08EA</td>
<td>65K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.32.18</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>08EC</td>
<td>1463K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.208.208</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0411</td>
<td>8351K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.77.66</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>126F</td>
<td>1763K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.184.159</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0609</td>
<td>191K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.22.48</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0885</td>
<td>1520K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.22.48</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0883</td>
<td>66K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.7.44</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0F07</td>
<td>97K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.7.44</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0F09</td>
<td>2084K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.54.208</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>040C</td>
<td>3018K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.248.90</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>0521</td>
<td>201K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.201.177</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>060C</td>
<td>171K</td>
</tr>
<tr>
<td>Hs9/1/0</td>
<td>192.168.201.177</td>
<td>Null</td>
<td>1.1.1.1</td>
<td>11</td>
<td>054C</td>
<td>107K</td>
</tr>
</tbody>
</table>

etc. . .
WHAT EXACTLY ARE YOU LOOKING FOR?

- As much fun as it is to just dig through the data, you tend to have a purpose for looking through it
  - The purpose of your analysis will drive the manner of your analysis
- Bots / malware
- Data exfiltration
- Policy violations
- Performance / utilization
FINDING BOTS

- Look for traffic on standard bot/malware ports
  - TCP/UDP 53
  - 6666, 6667 (IRC)
- Hard to find port 80 bots, but not impossible
  - Look for large # of connections with little bandwidth used
- Examine destination address… might want to look for data going to places you don’t trust
  - http://www.apnic.net/db/min-alloc.html
DATA EXFILTRATION

- Heavy outbound vs inbound data
  - 2:1 is a pretty good ratio to weed out the noise
  - In many non-academic environments, that’s sufficient…
- May need to rule out mail hosts and VPN gateways
  - They tend to be big outbound talkers
- Ex: 2000 hosts, might see 20 flows a day that hit this ratio
POLICY VIOLATIONS

- Known bad patterns
  - Hard to track P2P/VOIP traffic – Best to look for lots of src ports talking to lots of dst ports
- Have to get a good “eye” for what’s in your policy and how it manifests itself in your traffic
- Top talkers
  - GB of data a day, every day starts to seem fishy
- Where are your sensors?
  - If it’s just on the WAN links, you’ll miss internal violations… be sure you know where your data is coming from
PERFORMANCE / UTILIZATION

- Check out low speed links and inter-router connections
  - Obviously, look for pipes near capacity
  - Get an understanding of the types of data on the links and monitor the different types over time

- Top talkers
  - Figure out who and why

- High packet count / low packet sizes can indicate latency sensitive protocols
  - Talk to users about their experiences
BUILDING A COLLECTION AND ANALYSIS HOST

- Analysis of flows can be very intensive
  - Data tends to get stirred on the way in, and that takes CPU and disk
  - The queries by the user can get pretty whacky, and that takes CPU, disk, AND memory

- As a point of reference, a 2000 host organization will generate about 10M flows in a day.
  - That’s about 5k flows per host/day. A decent rule of thumb
  - ShmooCon had about 2M flows in a day and a half on about 150 machines
SCOPING A COLLECTION MACHINE

- You can do it on the sorta cheap if you want
  - Box 1 - Quad core, 3GB RAM, 500GB disk. $750
  - Box 2 - Quad core, 2 GB RAM, 400GB disk. $550
  - Extras - 3GB RAM($60), 2x500GB disk for RAID0 ($240)
  - $1500 == 2 super computers under my desk
INSTALLING PSYCHE

- Pretty easy. Download from http://psyche.pontetec.com/ and follow the directions
- DB == postgres. It’s different than MySQL, but doesn’t have the strange license issues.
- Primary testing is done against softflowd, but should work with any sensor.
Psyche - Network Flow Analysis for the Masses

There was a time when our anti-virus, IDS, and anti-spyware software could protect us from the majority of threats against our networks and systems. Unfortunately, the threats have changed, and our systems are getting compromised at an alarming rate. New tools are needed to help find attackers and malware on the network.

Psyche is a tool designed to utilize information already available in your network. Most modern routers and some switches can export network flow data that includes information on source and destination IP addresses and ports as well as size of the flows and number of packets sent. By performing analysis of this data, you can find out what is normal for your network and what is potentially dangerous traffic. For more information visit our website.

![Graphs showing network flow analysis](image)
Psyche - See more than just the tip of the Iceberg

Time Series

You selected: 2008-02-14 to 2008-02-29 23:59:59
Port Range: 1024 to 65535
Internal Net: 192.168.114.0/24

Graph Selection  Clear Selection

Note: Highlighting a portion of the graph allows you to drill down.

Aggregate Flow Information

<table>
<thead>
<tr>
<th>Interval</th>
<th>Src Addr</th>
<th>Dat Addr</th>
<th>Proto</th>
<th>Src Port</th>
<th>Dat Port</th>
<th>In Flows</th>
<th>Out Flows</th>
<th>In Packets</th>
<th>Out Packets</th>
<th>In Octets</th>
<th>Out Octets</th>
</tr>
</thead>
</table>
PARTING THOUGHTS

- We’re really just scratching the surface here
  - There are more tools, more views, more data to look at
  - For more tools, take a look at http://www.networkuptime.com/tools/netflow/
  - Really, all of these tools have the most relevance on your own network
    - You won’t believe the number of “ah-ha” moments you’ll have using NetFlow tools
  - You really don’t need a huge box to use the RRD-based tools
    - Take a spare system off the rack and fire up NFSen. Shouldn’t take more than an afternoon to configure
CONTACT INFO

Bruce Potter
bpotter@pontetec.com