



Snort GUIs: Acid, Snort Center, and Beyond

Mike Poor
mike@digitalguardian.net



What to do with all that data?

- Scenario: You've deployed 7 sensors
 - Primary IDS
 - Tailored IDS for web farm, email gateway, DNS servers
 - Internal IDS deployed on span ports monitoring HR vlan, Accounting vlan, and Development vlan from internal attacks.
- Problem: How do you manage them?
- Problem2: How do you analyze the data?

What we have here is a mock scenario. We have seven sensors, monitoring our corporate network. We like the idea of managing the sensors on the command line, but the bosses want more ROI. They like the idea that you know what your doing on the command line, but want reports, perhaps graphs. Some managers actually want to log in to some sort of console and understand something they are seeing.

To solve these management dilemma's, we look towards GUI's for snort. For the purpose of this presentation, we will concentrate only on free, open source GUI's.



Tools covered

■ Tools

- Snortsnarf – HTML alert sumarizer
- cerebus – speed driven alert correlator
- Acid – defacto standard web based console
- Snortcenter – Management and analysis



SnortSnarf

- Available under GPL from Silicon Defense:
www.silicondefense.com/products/freesoftware/snortsnarf/
- Organizes snort alerts in to HTML files, for easy browsing
- Pull architecture, great for post mortem analysis

Snort GUIs

© 2003 Mike Poor

Snortsnarf is available from: www.silicondefense.com/products/freesoftware/snortsnarf/

Simple to install, just download to the directory where you want it to work. You must have the following perl module installed:

<http://search.cpan.org/author/MUIR/Time-modules-2003.0211/>

Then all you need to do at a simplistic view is: `perl snortsnarf.pl alert`



SnortSnarf start page

All Snort signatures

SnortSnarf v021111.1

[Signature section \(11091\)](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

11091 alerts found using input module SnortFileInput, with sources:

- alert

Earliest alert at **08:00:39** 792061 on 06/02/2002
Latest alert at **07:35:07** 022061 on 06/02/2003

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	spp_stream4: TCP TOO FAST RETRANSMISSION WITH DIFFERENT DATA SIZE (possible fragroute) detection	3	2	1	Summary
N/A	spp_stream4: TTL EVASION (reassemble) detection	4	2	2	Summary
N/A	spp_stream4: possible EVASIVE RST detection	466	91	29	Summary
N/A	spp_stream4: TCP CHECKSUM CHANGED ON RETRANSMISSION (possible fragroute) detection	920	11	227	Summary
N/A	spp_stream4: Multiple Aacked Packets (possible fragroute)	5072	38	26	Summary
3	X11 outbound client connection detected [sid] [arachNIDS]	127	4	2	Summary
2	WEB-MISC http directory traversal [sid] [arachNIDS]	1	1	1	Summary
2	WEB-CGI bash access [www.cert.org] [sid] [CVE]	1	1	1	Summary

Snort GUIs

© 2003 Mike Poor

Here we see the index.html page after a snortsnarf pass on a snort alert file. Snortsnarf displays alerts based on Signature. The main columns are: Priority, Signature, # Alerts, # Sources, # Dests, Detail link.

By clicking on Signature, snortsnarf displays details regarding the rule. By clicking on Detail link you will drill down to the event information.



SnortSnarf Summary Detail

These are different IP's that are scanning our network for port 8080, looking for open proxies.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
218.75.141.14	24	24	8	8
192.168.1.17	20	273	3	101
218.75.141.10	11	11	8	8
62.224.46.122	7	14	7	7
192.168.1.2	1	79	1	22

Snort GUIs

© 2003 Mike Poor

Priority	Signature (click for sig info)	# Alerts	#
Sources	# Dests	Detail link	
2	SCAN Proxy (8080) attempt [sid]	63	5
	9	Summary	

Here we see detail of the port 8080 events. We see all the different sources that generated this alert, with statistics on how many signatures they've fired, how many destinations they have hit, and how many total alerts they have generated.

This is useful as we can quickly see that while a host on our internal network is the biggest culprit, 218.75.141.14 is only scanning for port 8080.

A click on the IP address will show all events attributed to this IP address.

Attackers often use open proxies to 'bounce' attacks off of. They also use open proxies for anonymous web browsing.



Snortsnarf Target Detail

This section displays the target distribution for this alert.

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
192.168.1.7	15	531	4	31
192.168.1.10	14	1176	4	53
192.168.1.4	7	326	3	33
192.168.1.5	7	1459	4	349
192.168.1.6	5	995	3	109
192.168.1.9	5	233	3	11
192.168.1.8	5	228	3	10
192.168.1.15	4	4	2	2
192.168.1.2	1	8	1	2

Here we can see the overall distribution of targets for this alert. We see that 192.168.1.5 is by far the greatest target for this event.

From here we can drill down to the IP address and see the different events that are affecting a particular IP address.



SnortSnarf Event Detail

```
[**] [1:620:2] SCAN Proxy (8080) attempt [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/27-22:26:09.677260 218.75.141.14:1532 -> 192.168.1.6:8080  
TCP TTL:110 TOS:0x0 ID:49152 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0xC6576163 Ack: 0x0 Win: 0x4000 TcpLen: 28  
TCP Options (4) => MSS: 1460 NOP NOP SackOK  
  
[**] [1:620:2] SCAN Proxy (8080) attempt [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
05/27-22:26:09.687260 218.75.141.14:1528 -> 192.168.1.4:8080  
TCP TTL:110 TOS:0x0 ID:49148 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0xC6541DEB Ack: 0x0 Win: 0x4000 TcpLen: 28  
TCP Options (4) => MSS: 1460 NOP NOP SackOK
```

- Details of attacks coming from 218.75.141.14
- Only one signature, with 24 instances, 8 unique destinations on our network.

1 different signatures are present for 218.75.141.14 as a source

* 24 instances of SCAN Proxy (8080) attempt

There are 8 distinct destination IPs in the alerts of the type on this page.

Here we could also run a number of information gathering tools against the attacker, including: whois, nslookup, sam spade, as well as looking up the attacker in Dshield's database. This last item can be very useful to see if this IP address is indeed scanning the Net for open proxies, and not just our network.



SnortSnarf Top Attackers

Rank	Total # Alerts	Source IP	# Signatures triggered	Destinations involved
rank #1	5361 alerts	192.168.1.5	6 signatures	(86 destination IPs)
rank #2	1002 alerts	64.50.195.73	2 signatures	(4 destination IPs)
rank #3	945 alerts	64.50.195.130	3 signatures	(6 destination IPs)
rank #4	273 alerts	192.168.1.17	8 signatures	(101 destination IPs)
rank #5	257 alerts	66.38.151.27	1 signatures	192.168.1.5
rank #6	203 alerts	192.168.1.30	2 signatures	(55 destination IPs)
rank #7	153 alerts	12.33.247.3	2 signatures	192.168.1.5
rank #8	150 alerts	192.168.1.4	5 signatures	(18 destination IPs)
rank #9	135 alerts	64.133.161.40	2 signatures	(5 destination IPs)
rank #10	102 alerts	64.154.220.122	1 signatures	(6 destination IPs)

- Provides an easy method of discerning the current external threat
- Great fodder for your block lists

In using SnortSnarf as a quick, pull based “summarizer” or snort reporting tool, an analyst can quickly drill down to some of the more important events on the network.



SnortSnarf Pros & Cons

Pros

- Free
- Ease of install
- Simple to use
- Overall picture
- Good management tool

Cons

- Slow to process large alert files
- Can produce thousands of HTML files
- Does not show event detail (packets)



Cerebus

<http://www.dragos.com/cerebus/>

“Full screen, GUI and text-based unified
IDS alert file browser and data
correlator”

- Cerebus is a fast, lean, unified alert
munching machine

Cerebus is an interesting beast. Written by Dragos Ruiu, cerebus is a curses based Alert browser and correlator. Cerebus allows the user to upload a snort unified binary alert file, view, sort, collapse, delete, and merge alerts. What Cerberus excels at is alert triage. If you are an admin on a large network, and are further burdened by having to go through thousands of snort alerts a day, cerberus could be the tool of choice for you.



Cerebus Install

- Cerebus is downloaded in executable binary form.
- Choose the platform that suits your environment
- Available for:
 - Unices: *BSD, Solaris, Linux
 - Win32

Cerebus is shareware. In order to get full version, or to use Cerebus in an enterprise, contact Dragos at: dr@dursec.com for licensing.



Cerebus Operation

- First you must enable unified binary alerting / logging in snort.conf:

output alert_unified: filename snort.alert, limit 128

output log_unified: filename snort.log, limit 128

Usage: ./cerebus <filename> [/path/to/sid-msg.map] [outfile]

- Example:

./cerebus snort.alert /etc/snort/etc/sid-msg.map foo.out

Enable snort unified binary logging and alerting by setting the following lines in snort.conf:

output alert_unified: filename snort.alert, limit 128

output log_unified: filename snort.log, limit 128



Snort GUIs

© 2003 Mike Poor



Cerebus Operation

■ Main actions:

- (C)ollapse
- (E)xpand
- (S)ort – IP (src|dst), Event,
- (D)elete
- (R)emove
- (M)erge
- (W)rite

Snort GUIs

© 2003 Mike Poor

(C)ollapse (E)xpand (S)ort (D)el (R)emove (M)erge (W)rite (Q)uit

Collapse: (S)ource (D)estination (A)lert (P)riority (C)lass

Sort: (T)ime (S)ource (D)est. (A)lert (P)rio. (C)lass (E)vent

Collapse will show you all your alerts based on source, destination, alert, priority or class. You can also sort the alerts by Time, source, destination, alert, priority, class, or event.

These are very useful for culling events. Say you have 145676 events regarding cmd.exe access. You are a Unix only shop, and have verified this in your hourly baseline scan. Collapse all alerts based on alert (C) + (A), then highlight the cmd.exe access alert line, and delete them. You have just removed almost 150K events, with three clicks.



Cerebus Collapse | Delete

No of 10001(01)		Cipst810		Sort810-EVN		CEREBUS V1.4L		Files: 1		Output:foo.out		SID-Hap:sort-2,0,0/etc/sid-wsg-map		SID	
Count	Time/Sec	Source IP	Port	Dest IP	Port	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert
15710	W	192.168.1.2	1	192.168.1.17	1	SID 8	5	Not Suspicious	W	8					
19	W	192.168.1.2	1	192.168.1.17	1	SID 9	5	Not Suspicious	W	9					
7	W	192.168.1.2	1	192.168.1.17	1	SID 10	5	Not Suspicious	W	10					
1	2/9	04110145.336935	192.168.1.2	1	192.168.1.17	0	SID 11	5	Not Suspicious	W	11				
1	2/9	04110145.316835	192.168.1.2	1	192.168.1.17	0	SID 12	5	Not Suspicious	W	12				
11	W	192.168.1.2	1	192.168.1.17	0	SID 13	5	Not Suspicious	W	13					
1	2/9	04126105.036835	192.168.1.2	1	192.168.1.17	0	SID 14	5	Not Suspicious	W	14				
1	2/9	04110145.676935	192.168.1.2	1	192.168.1.17	0	SID 15	5	Not Suspicious	W	15				
1	2/9	04110130.216835	192.168.1.2	1	192.168.1.17	0	SID 16	5	Not Suspicious	W	16				
1	2/9	04119108.616835	192.168.1.2	1	192.168.1.17	0	SID 17	5	Not Suspicious	W	17				
1	2/9	04125130.676935	192.168.1.2	1	192.168.1.17	0	SID 18	5	Not Suspicious	W	18				
3	W	192.168.1.2	1	192.168.1.17	0	SID 19	5	Not Suspicious	W	19					
16	W	192.168.1.2	1	192.168.1.17	0	SID 20	5	Not Suspicious	W	20					
9	W	192.168.1.2	1	192.168.1.17	0	SID 21	5	Not Suspicious	W	21					
29	W	192.168.1.2	1	192.168.1.17	0	SID 22	5	Not Suspicious	W	22					
17	W	192.168.1.2	1	192.168.1.17	0	SID 23	5	Not Suspicious	W	23					
14	W	192.168.1.2	1	192.168.1.17	0	SID 24	5	Not Suspicious	W	24					
2	W	192.168.1.2	1	192.168.1.17	0	SID 25	5	Not Suspicious	W	25					
2	W	192.168.1.2	1	192.168.1.17	0	SID 26	5	Not Suspicious	W	26					

Functions: Collapse Expand Sort Cbtl Overview George Write Quit

CEREBUS-1.4L-debug

- Using 3 keystrokes, we can process a good majority of our alerts
- Gives the analyst the time to focus on important events



Cerebus Pros and Cons

Pros

- Fast
- Curses based for easy shell access
- Cross Platform
- Good tool for Alert triage

Cons

- Not free for all uses
- Not a "managers" tool
- Must be savvy to use
- No event detail yet
- No support for pcap files yet



Analysis Console for Intrusion Databases

www.andrew.cmu.edu/~rdanyliw/snort/snortacid/

- Free - Distributed under the GPL
- PHP web based console
- Defacto standard web based front end for snort alert analysis

Acid Screenshot

Analysis Console for Intrusion Databases (ACID) - Mozilla

Added 0 alert(s) to the Alert cache

Queried on: Mon Jun 02, 2003 11:10:28
Database: snort_db@localhost (schema version: 106)
Time window: no alerts detected

Sensors: 0
Unique Alerts: 0 (0 categories)
Total Number of Alerts: 0

- Source IP addresses: 0
- Dest. IP addresses: 0
- Unique IP links: 0
- Source Ports: 0
 - TCP (0) UDP (0)
- Dest. Ports: 0
 - TCP (0) UDP (0)

Traffic Profile by Protocol

- TCP (0%)
- UDP (0%)
- ICMP (0%)
- Portscan Traffic (0%)

Search
Graph Alert data
Snapshot

- Most recent Alerts: any protocol, TCP, UDP, ICMP
- Today's alerts unique, listing: IP src / dst
- Last 24 Hours alerts unique, listing: IP src / dst
- Last 72 Hours alerts unique, listing: IP src / dst
- Most recent 15 Unique Alerts
- Last Source Ports: any, TCP, UDP
- Last Destination Ports: any, TCP, UDP
- Most frequent 5 Alerts
- Most Frequent Source Ports: any, TCP, UDP
- Most Frequent Destination Ports: any, TCP, UDP
- Most frequent 15 addresses: source, destination

Graph alert detection time
Alert Group (AG) maintenance
Application cache and status

[Loaded in 1 seconds]

ACID v0.9.6a23 (by Norman Danyliw as part of the AirCER project)

Snort GUIs © 2003 Mike Poor

Acid's main screen. Acid allows one to query a database of event information for specific data. One can query the db for all events from a range of time, from a specific IP address, or specific event and so on.



Acid Install

- You will need:
 - acid
 - gd
 - jpgraph
 - mysql
 - Apache and PHP
 - snort / barnyard / lognorter

First of all, you will need snort, barnyard or lognorter, in order to get information into the database.

Then you will need the database, in this case mysql.

Followed by apache and PHP, with gd and jpgraph libraries installed.



Acid install continued

■ Install the database

- `mysql -u root -p < create_mysql`
- `mysql -u root -p < create_acid_tbls_mysql.sql`

■ Grant privileges to your db user

- `GRANT ALL ON snort_db TO acid_user IDENTIFIED by "foo"`

■ Check database tables:

- `show tables;`
- check notes for tables:

Create db with the scripts in snort-2.0.0/contrib and acid-0.9.6x

```
+-----+
| Tables_in_snort_db |
+-----+
| acid_ag            |
| acid_ag_alert      |
| acid_event         |
| acid_ip_cache      |
| data               |
| detail             |
| encoding           |
| event              |
| icmphdr            |
| iphdr              |
| opt                |
| reference           |
| reference_system   |
| schema             |
| sensor             |
```



Barnyard Install

- Available from:
<http://www.snort.org/dl/barnyard/>
- Barnyard was developed to decouple the output process from snort
- To install:
`./configure && make && make install`

Barnyard was developed to decouple the output process from snort. Barnyard is released under the QPL license, and is available from: <http://www.snort.org/dl/barnyard>

The Barnyard process is niced, running at a lower priority than snort, and processes snort unified binary files.

The main process for snort to work is to enable



Snort & Barnyard

- Set up snort.conf to log in unified binary mode:
 - output alert_unified: filename snort.alert, limit 128
 - output log_unified: filename snort.log, limit 128
- Set up barnyard.conf to log to mysql
 - output log_acid_db: mysql, database snort_db, server localhost, user root, detail full, password foo

Snort GUIs

© 2003 Mike Poor

snort.conf

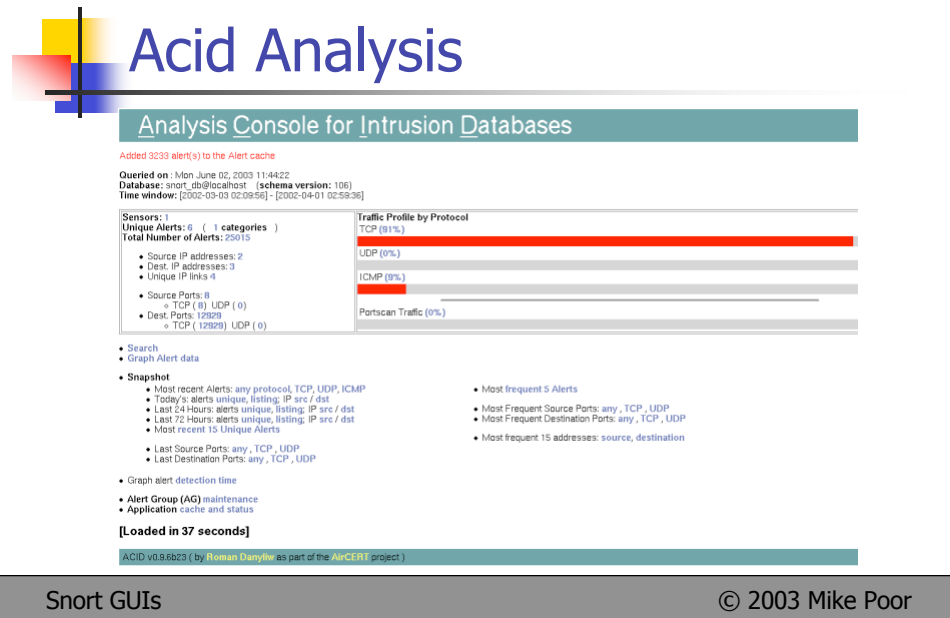
output alert_unified: filename snort.alert, limit 128

output log_unified: filename snort.log, limit 128

barnyard.conf

output log_acid_db: mysql, database snort_db, server localhost, user root, detail full, password foo

output alert_acid_db: mysql, sensor_id 1, database snort, server localhost, user root, password foo



Here we have the Acid console loaded with 25015 alerts. Notice that the report took 37 seconds to load



Acid Top reports

- Reporting helps prioritize analysis process
 - Top 5/15 alerts
 - Most recent alerts
 - Most frequent Ports (src | dst)
 - Most frequent Addresses (src | dst)
 - Today's alerts (unique | listing)



Acid Alert munging

ACID Alert Listing: 5 Most Frequent Alerts [Home](#) [Search](#) [AG Maintenance](#) [\[Back \]](#)

Added 0 alert(s) to the Alert cache

Queried DB on: Mon Jun 02, 2003 11:52:48

Meta Criteria	any
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

Displaying 5 Most Frequent Alerts

	Signature	Classification	Total #	Sensor #	Src. Addr.	Dest. Addr.	First	Last
<input type="checkbox"/>	[snort] Snort Alert [1118:0]	unclassified	34597 (94%)	1	2	2	2002-03-03 02:12:43	2002-03-03 04:18:45
<input type="checkbox"/>	[snort] Snort Alert [1472:0]	unclassified	21378 (5%)	1	1	2	2002-03-29 17:18:17	2002-04-01 02:59:36
<input type="checkbox"/>	[snort] Snort Alert [1820:0]	unclassified	43 (0%)	1	3	11	2002-03-03 02:10:15	2002-03-03 11:42:01
<input type="checkbox"/>	[snort] Snort Alert [1618:0]	unclassified	35 (0%)	1	3	11	2002-03-03 02:10:15	2002-03-03 11:42:01
<input type="checkbox"/>	[snort] Snort Alert [1524:0]	unclassified	15 (0%)	1	2	2	2002-03-03 04:18:45	2002-03-03 04:23:46

{ action } Action Selected ALL on Screen

[Loaded in 7 seconds]

- Acid allows for basic data aggregation and sorting
- Can get slow for tens of thousands of alerts and above



Acid Pros and Cons

Pros

- Free, GPL
- Well documented
- Full web based front end for snort
- Designed for analysis

Cons

- Slow
- resource intensive
- Heavy maintainance
- Does not scale to the enterprise level
- limited operation on events



SnortCenter

“Snort IDS Rule & Sensor Management”

- Free from:
 - <http://users.pandora.be/larc>
- Web based front end multi-sensor management and analysis console
- User authentication, and SSL support for encrypting communication

Snort GUIs

© 2003 Mike Poor

<http://users.pandora.be/larc/>

Snortcenter is pushing fast to become the open source gui for the enterprise. Downloaded from the URL above.



Snortcenter requirements

- Install the following:

- apache w/ php
- mysql
- jpgraph
- curl
- openssl
- NET::SSLeay

from <http://users.pandora.be/larc> :

- # A working Webserver (apache) <http://httpd.apache.org/>
- # PHP Version: 4.2+ compiled with --with-mysql <http://www.php.net/>
- # MySQL Version: 3.23.x+ <http://www.mysql.com/>
- # cURL command line tool (with SSL support) <http://curl.haxx.se/>



Snortcenter install

- Two parts
 - www -> handles web console
 - sensor-agent -> manages sensors
- Unpack both tar balls into your htdocs directory
 - `tar zxvf snortcenter-agent-v1.0-x.tar.gz`
 - `tar zxvf snortcetner-v1.0-x.tar.gz`

The install comes with two parts. A web console section, and a sensor management section. If you are installing both parts on one machine, untar the packages in your htdocs directory of your webserver.



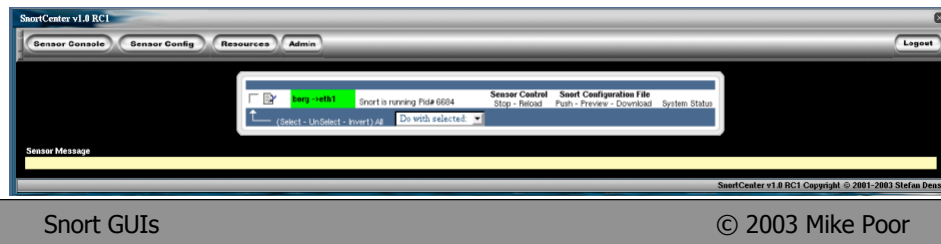
SnortCenter install

- Create the database
 - `mysql -u root -p < echo "CREATE DATABASE snortcenter;"`
 - `mysql -u root -p < snortcenter_db.mysql`
- Open browser to <http://localhost/> to load tables

Follow directions in INSTALL file for database installation.

SnortCenter Install

- Now set up sensor
 - in /<webdir>/sensor/ run the setup.sh script
- Add a sensor from <http://localhost/>



Now that you have configured your web console, its time to configure your sensor. The sensor can be added from <http://localhost/> by clicking on <Sensor Console><Add Sensor>



Snort Center Operation

- Use snortcenter to:
 - manage, tailor, and deploy rule sets
 - view alerts through the acid plugin
 - manage, start, stop, and view status of your sensors

A detailed guide to the installation of Snortcenter and all components ontop of a Red Hat 7.3. machine can be found at:

http://users.pandora.be/larc/documentation/snort_enterprise.pdf

Rule management



Rules template creation. Screenshot courtesy SnortCenter.

Here we can see snortcenter managing the tftp.rules for inclusion on this sensor.



SnortCenter Pros and Cons

Pros

- Free – GPL
- Cross platform, web based
- Central repository for rules, analysis, policy
- “Manager enabled”

Cons

- Slow
- No pcap support
- Resource intensive
- Lengthy install

Overall snortcenter is a very capable tool. It handles all aspects of snort management, from sensor deployment and tuning, to analysis and rule updates.



Wrapup

- Many free/opensource options available
 - simple command line processing
 - analysis via acid
 - management using snortcenter
 - alert processing with cerebus
- Choose the tool that is appropriate to your environment and snorting style.

For additional reading, I would recommend the PHP tutorial at:
<http://us2.php.net/tut.php>

a mysql book such as: MySQL by Paul Dubois

And the documentation provided by each of the tools mentioned in this presentation.