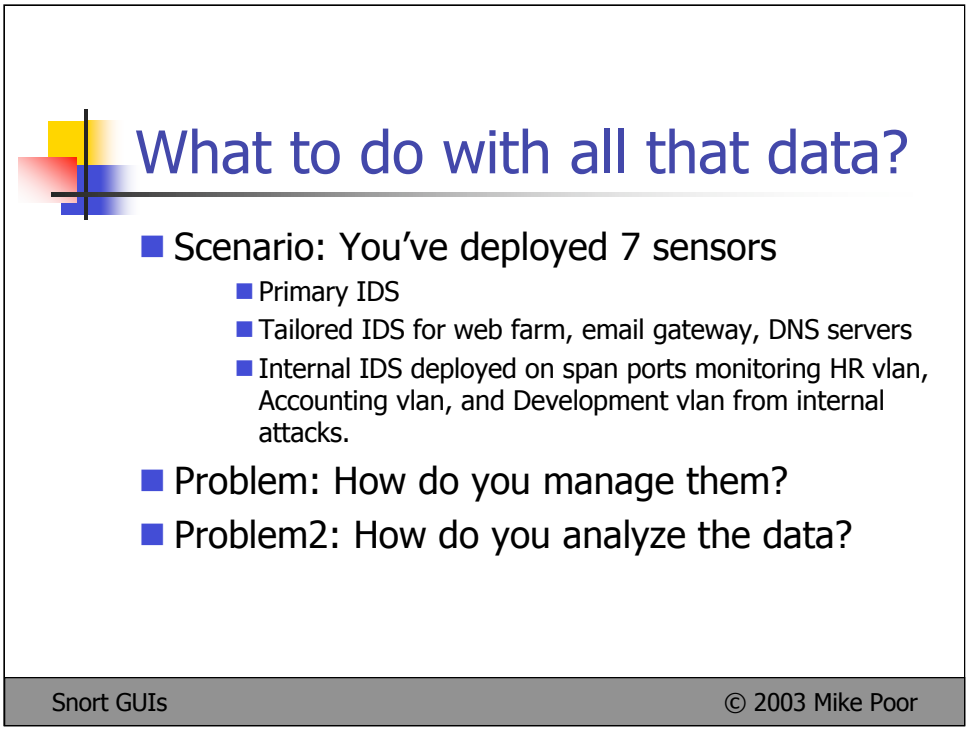
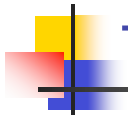
Snort GUIs: Acid, Snort Center, and Beyond

Mike Poor
mike@digitalguardian.net



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

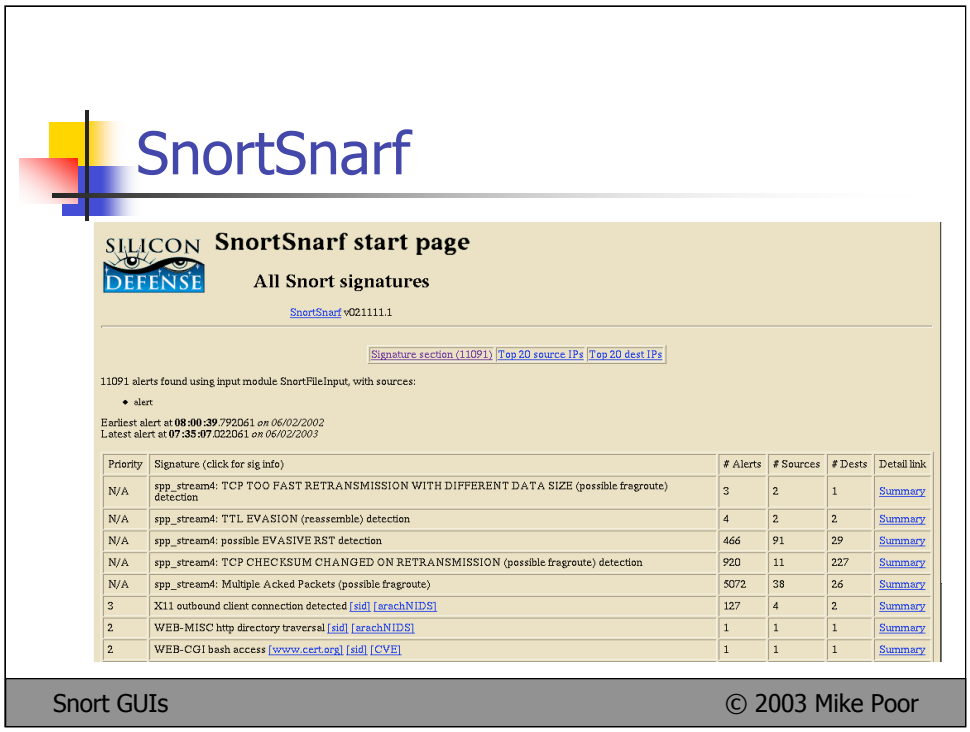
- Tools
  - Snortsnarf – HTML alert sumarizer
  - cerebus – speed driven alert correlator
  - Acid – defacto standard web based console
  - Snortcenter – Management and analysis

Snortsnarf is a 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

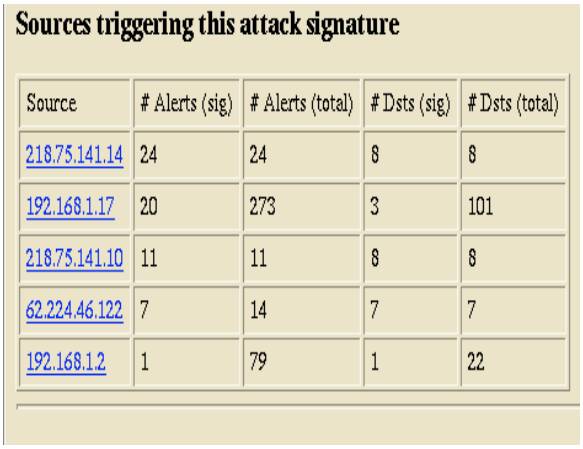


Here we see the index.html page after a snortsnarf pass on a snort alert file. Snortsnarf displays alerts based on Signature. The main columns are: Priority, Signature, # Alerts, # Sources, # Dests, Detail link.

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

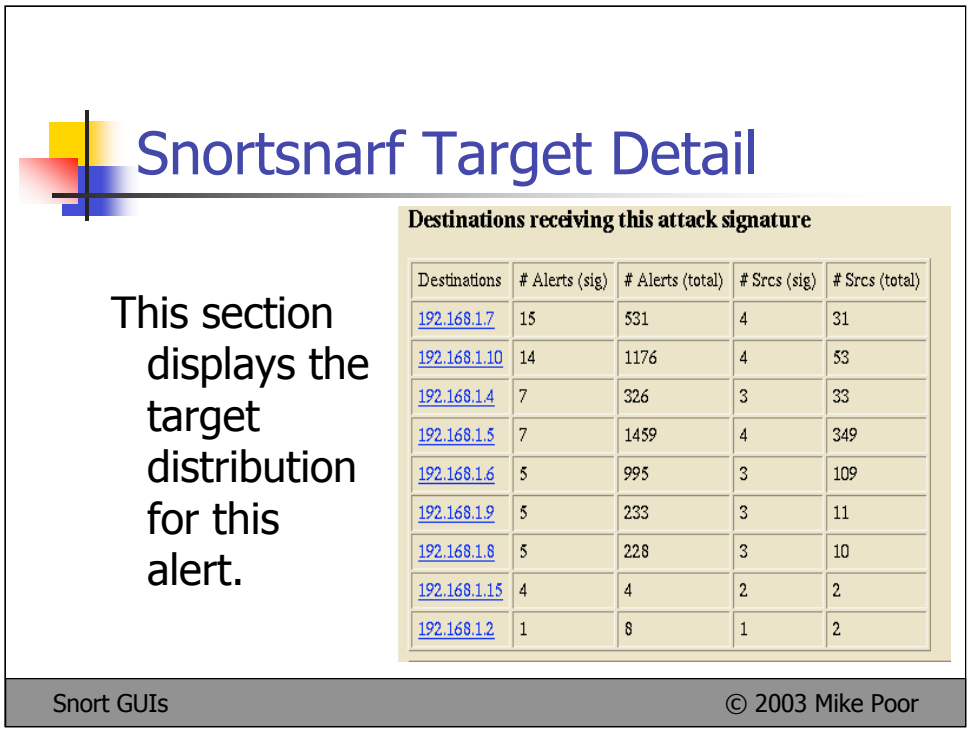
Priority	Signature (click for sig info)		# Alerts	# Sources	# Dests	Detail link
2	SCAN Proxy (8080) attempt [sid] 9	63	5			Summary

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.

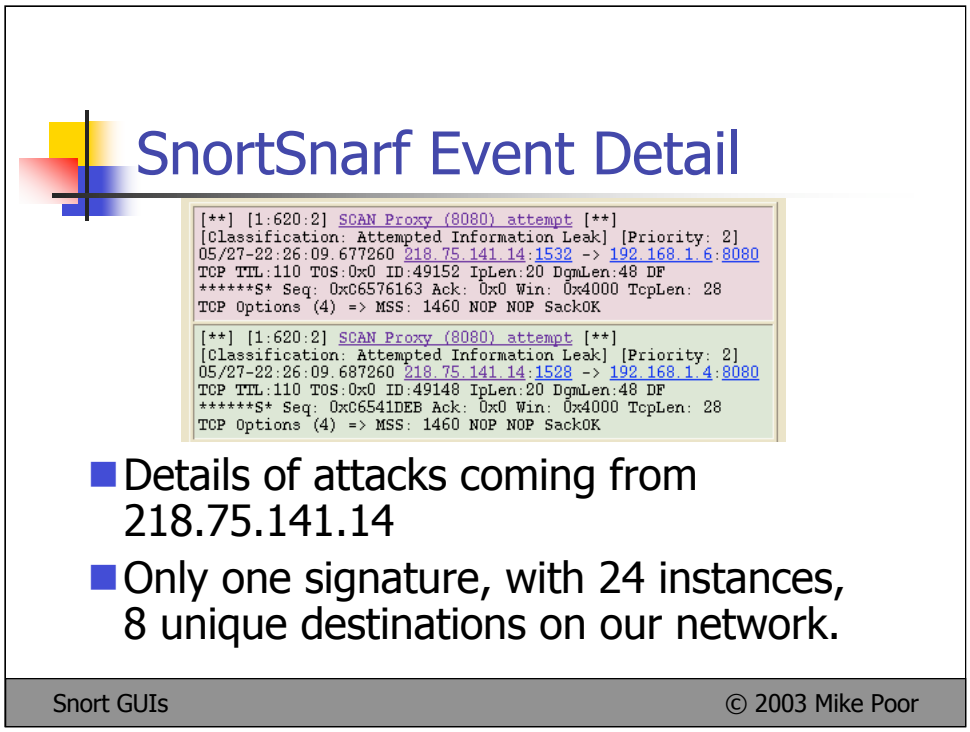
A click on the IP address will show all events attributed to this IP address.

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



Here we can see the overall distribution of targets for this alert. We see that 1921.68.1.5 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.

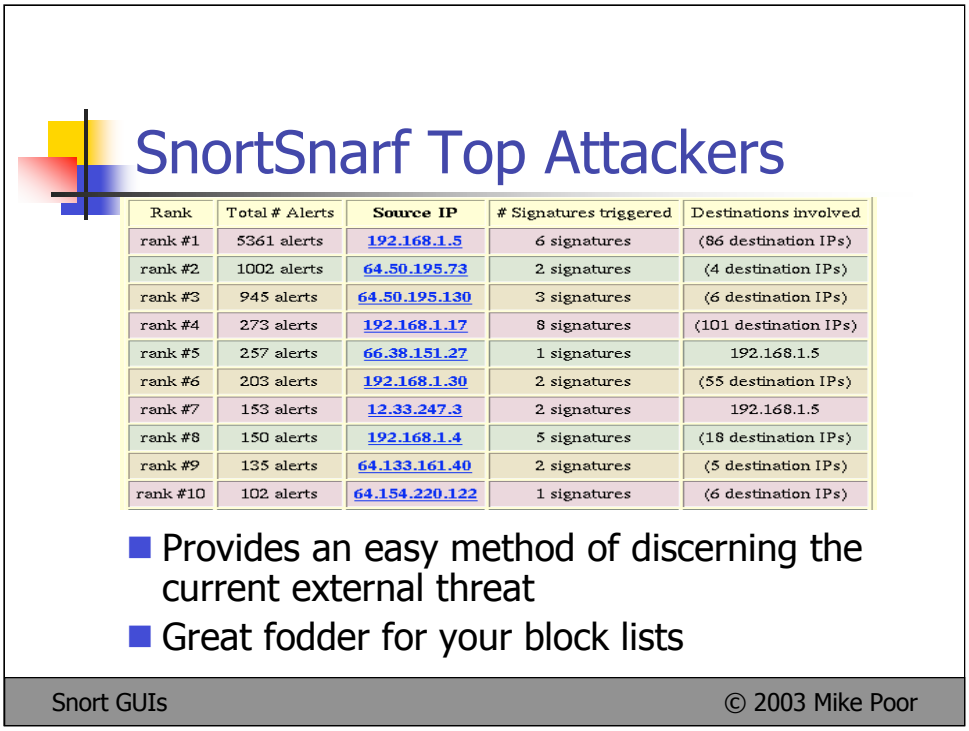


1 different signatures are present for 218.75.141.14 as a source

* 24 instances of SCAN Proxy (8080) attempt

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

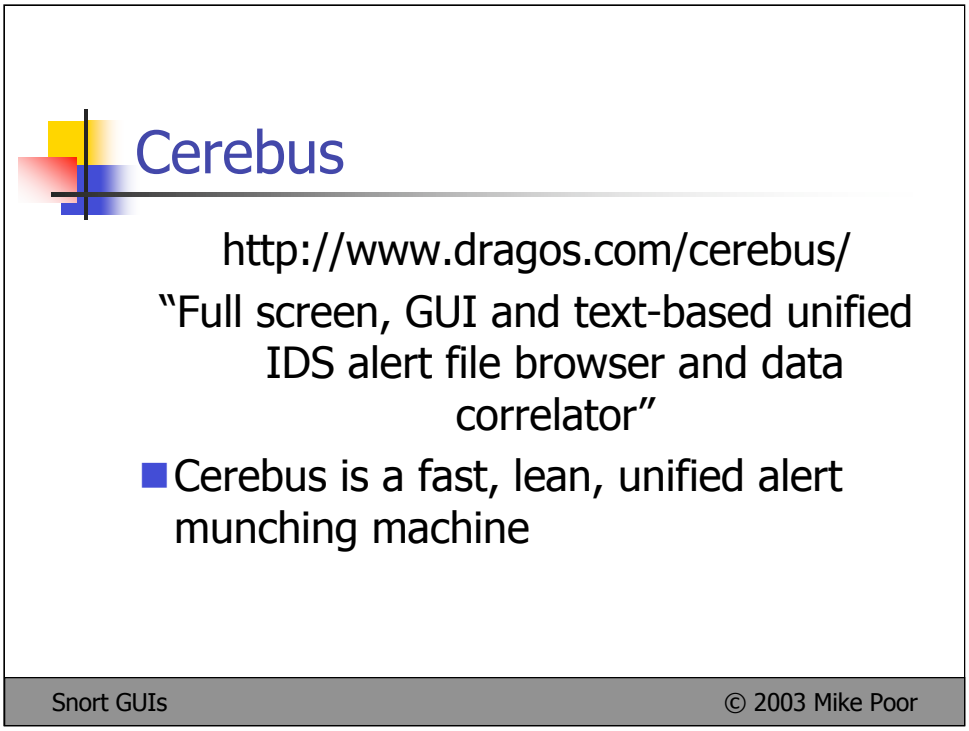
Here we could also run a number of information gathering tools against the attacker, including: whois, nslookup, sam spade, as well as looking up the attacker in Dshield's database. This last item can be very useful to see if this IP address is indeed scanning the Net for open proxies, and not just our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



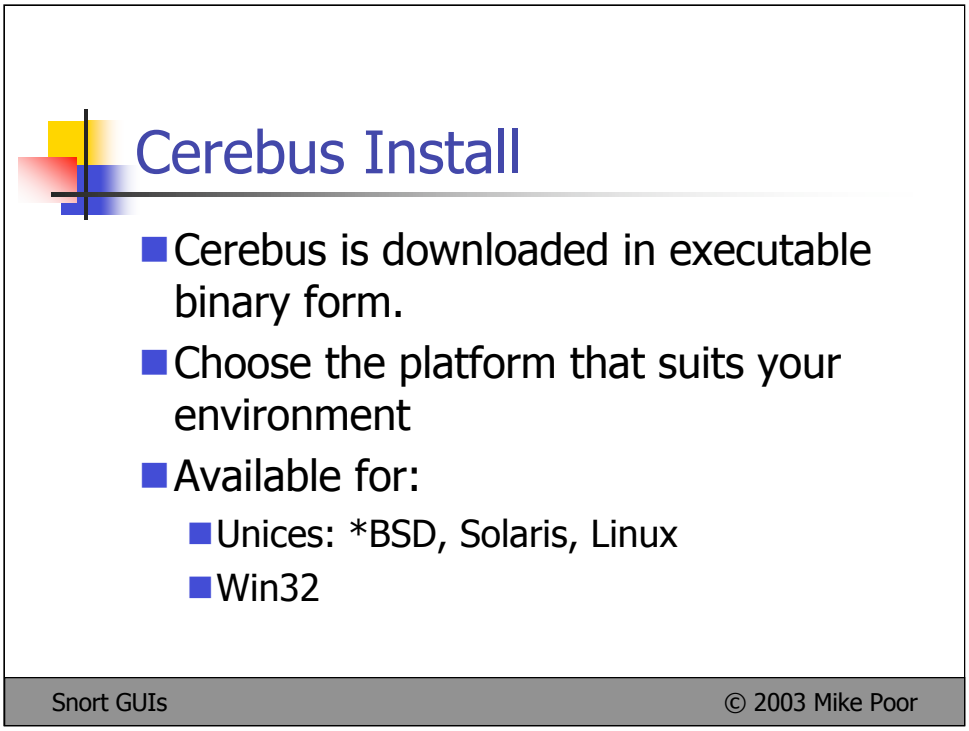
In using SnortSnarf as a quick, pull based “summarizer” or snort reporting tool, an analyst can quickly drill down to some of the more important events on the network.

SnortSnarf Pros & Cons

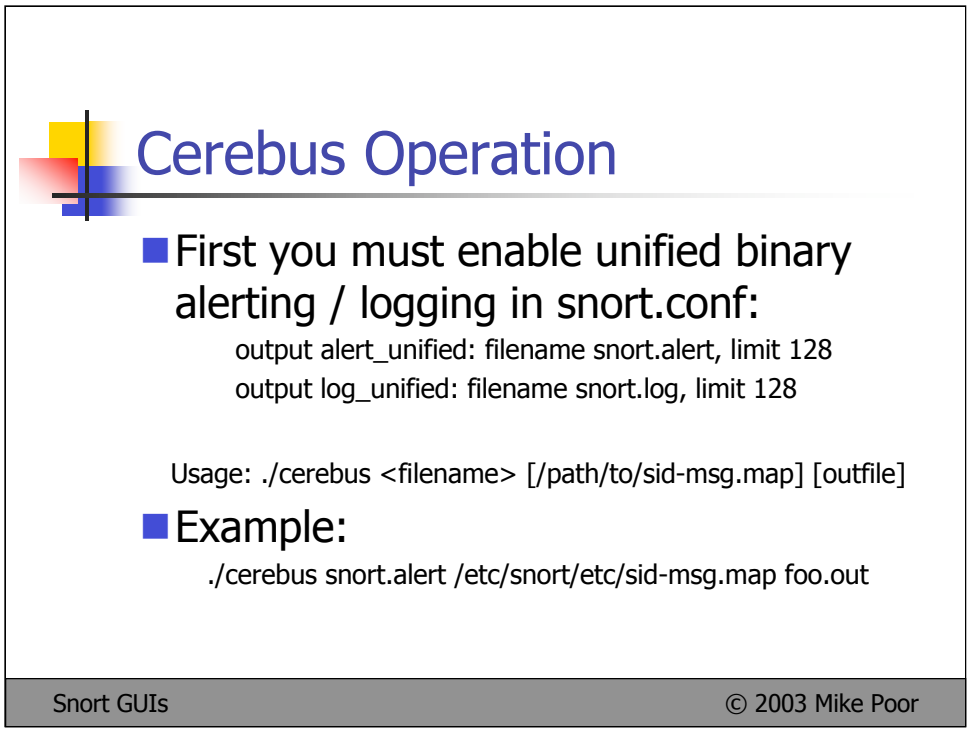
Pros	Cons
■ Free	■ Slow to process large alert files
■ Ease of install	■ Can produce thousands of HTML files
■ Simple to use	■ Does not show event detail (packets)
■ Overall picture	
■ Good management tool	



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

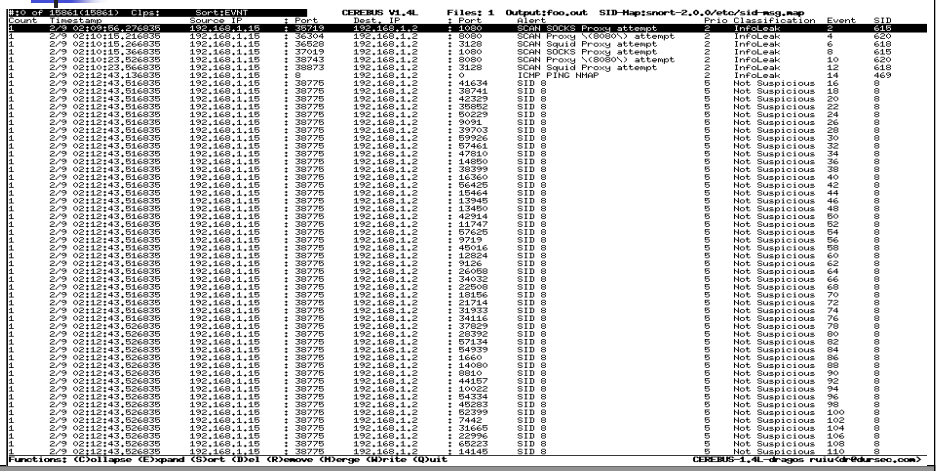


Enable snort unified binary logging and alerting by setting the following lines in snort.conf:

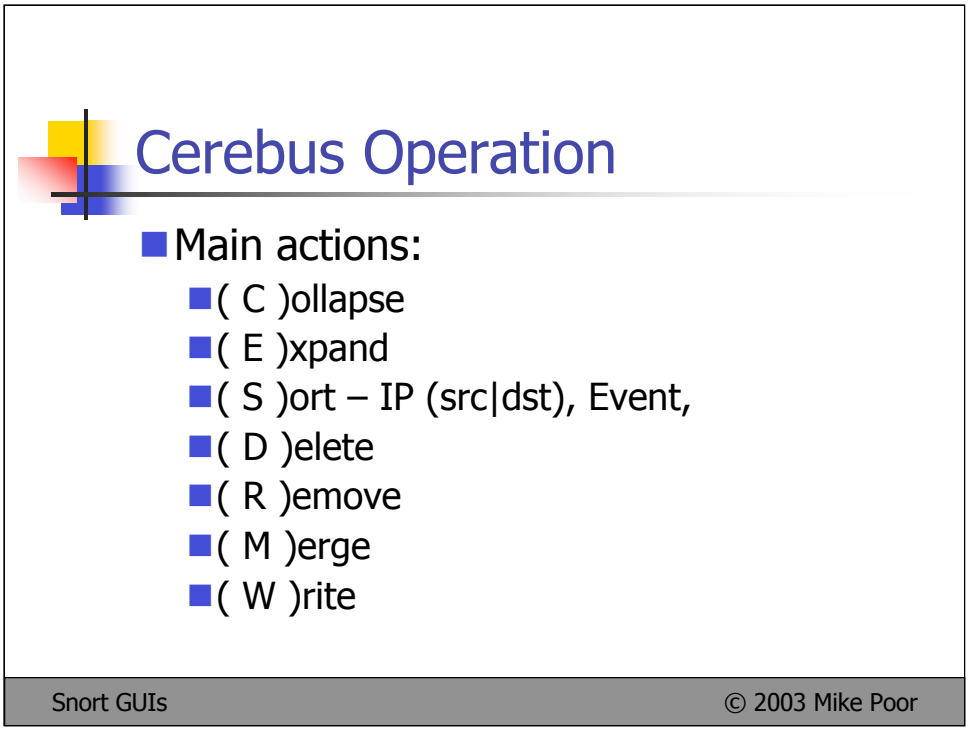
output alert_unified: filename snort.alert, limit 128

output log_unified: filename snort.log, limit 128

Cerebus



Snort GUIs



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

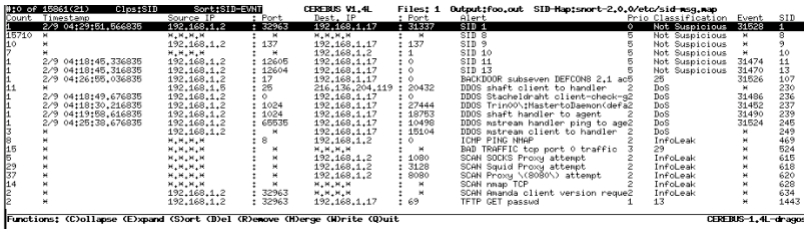
Collapse: (S)ource (D)estination (A)lert (P)riority (C)lass

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



- 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	Cons
■ Fast	■ Not free for all uses
■ Curses based for easy shell access	■ Not a "managers" tool
■ Cross Platform	■ Must be savvy to use
■ Good tool for Alert triage	■ No event detail yet
	■ No support for pcap files yet

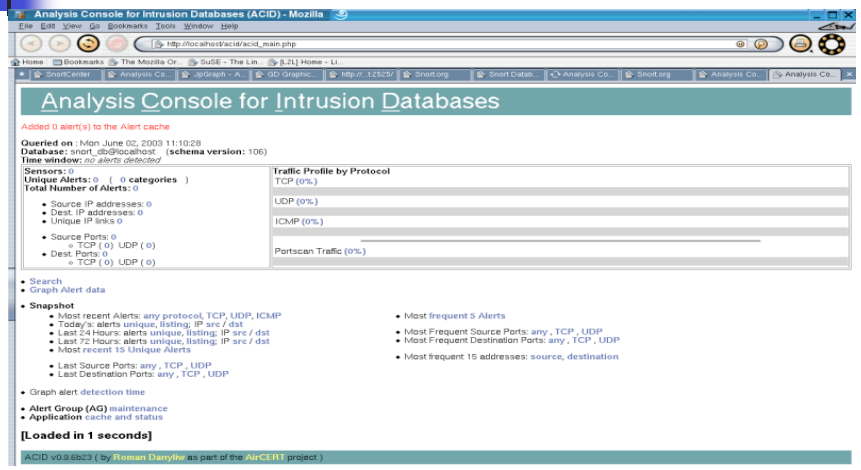
Acid

Analysis Console for Intrusion Databases

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

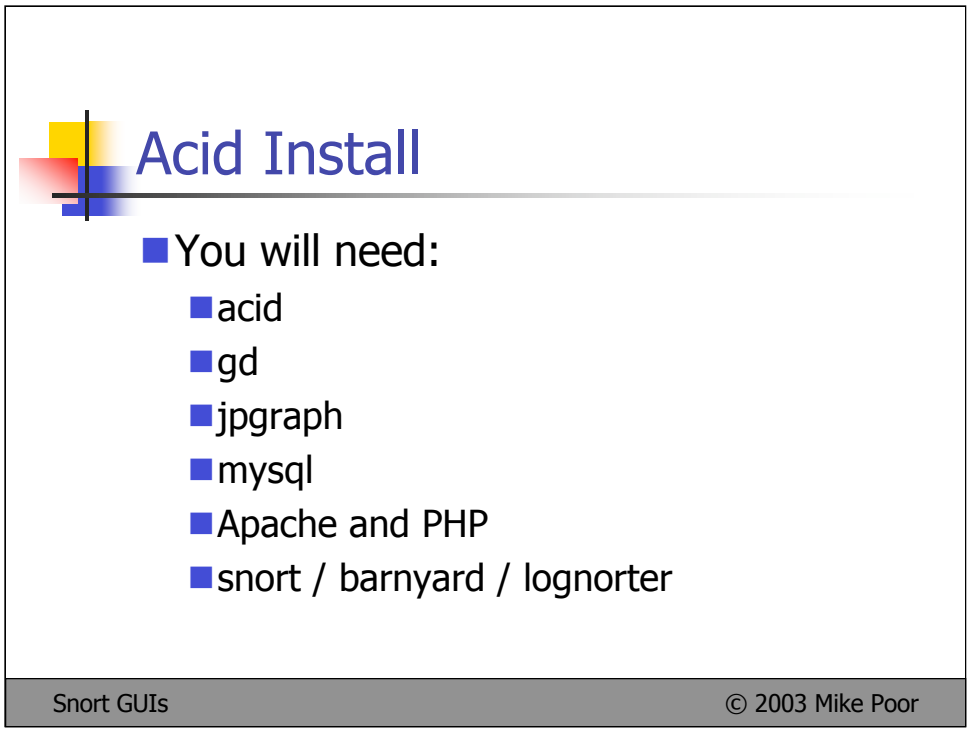
- Free - Distributed under the GPL
- PHP web based console
- Defacto standard web based front end for snort alert analysis

Acid Screenshot



Snort GUIs © 2003 Mike Poor

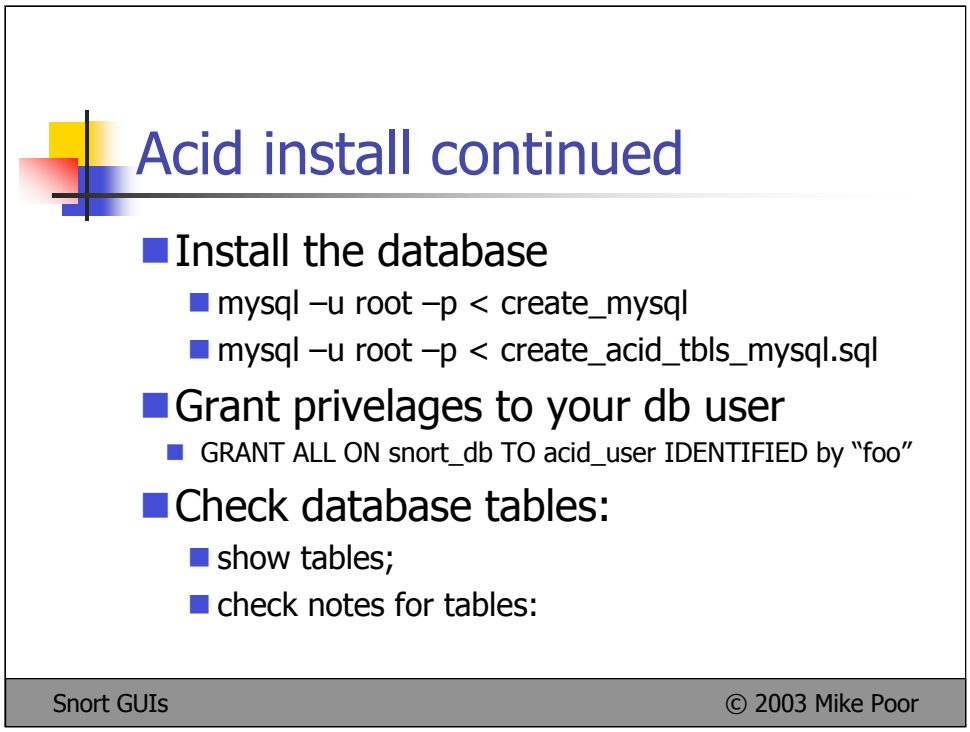
Acid's main screen. Acid allows one to query a database of event information for specific data. One can query the db for all events from a range of time, from a specific IP address, or specific event and so on.



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

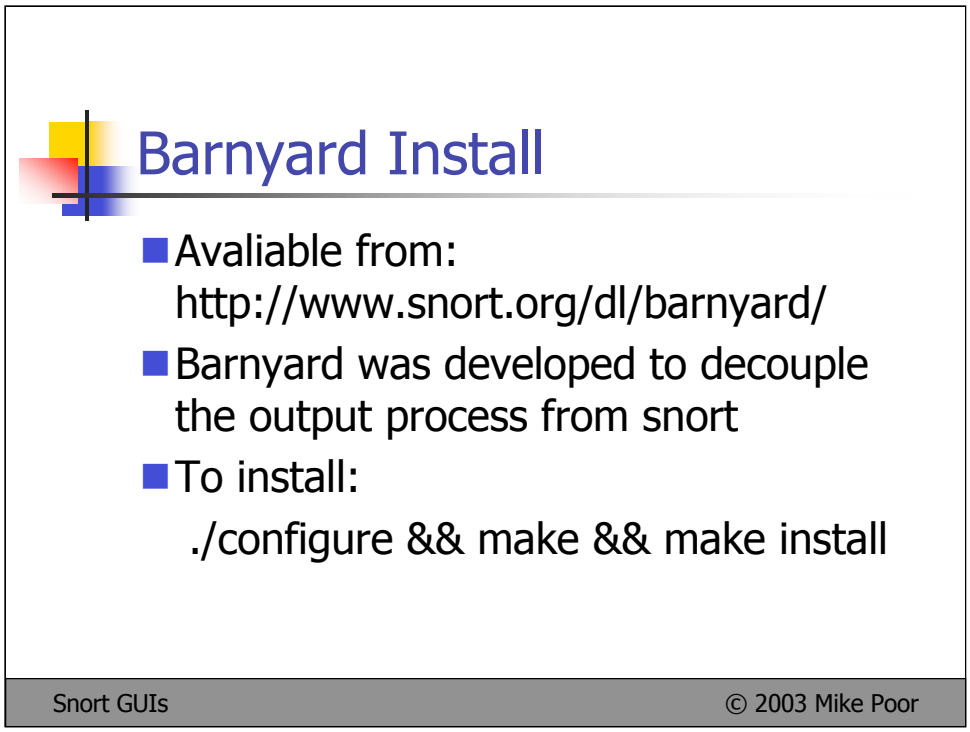
Then you will need the database, in this case mysql.

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



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

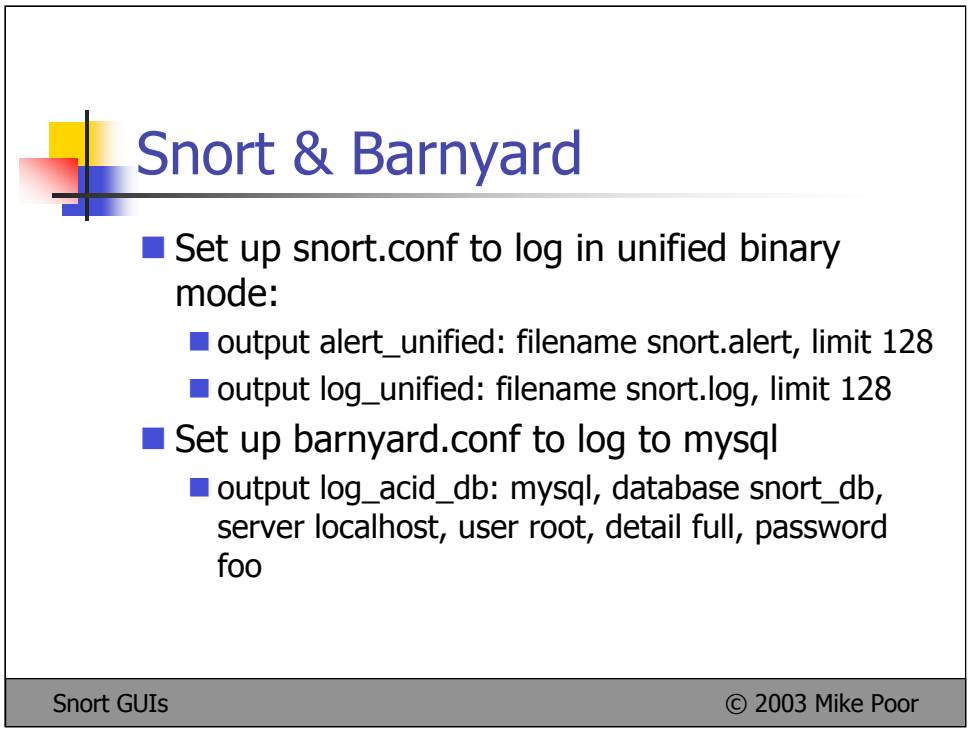
```
+-------------------+
| Tables_in_snort_db |
+-------------------+
| acid_ag           |
| acid_ag_alert     |
| acid_event        |
| acid_ip_cache     |
| data              |
| detail            |
| encoding          |
| event             |
| icmphdr           |
| iphdr             |
| opt    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



Barnyard 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 then snort, and process snort unified binary files.

The main process for snort to work is to enable



snort.conf

output alert_unified: filename snort.alert, limit 128

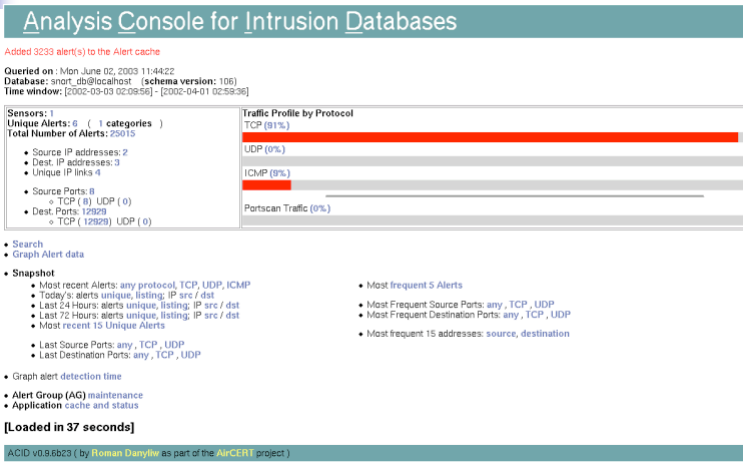
output log_unified: filename snort.log, limit 128

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

Acid Analysis

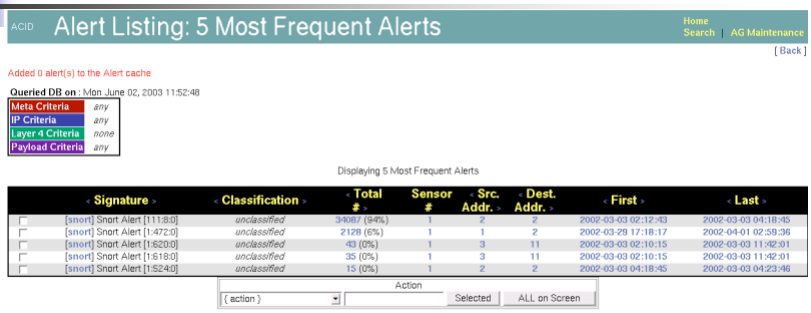


Here we have the Acid console loaded with 25015 alerts. Notice that the report took 37 seconds to load

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)

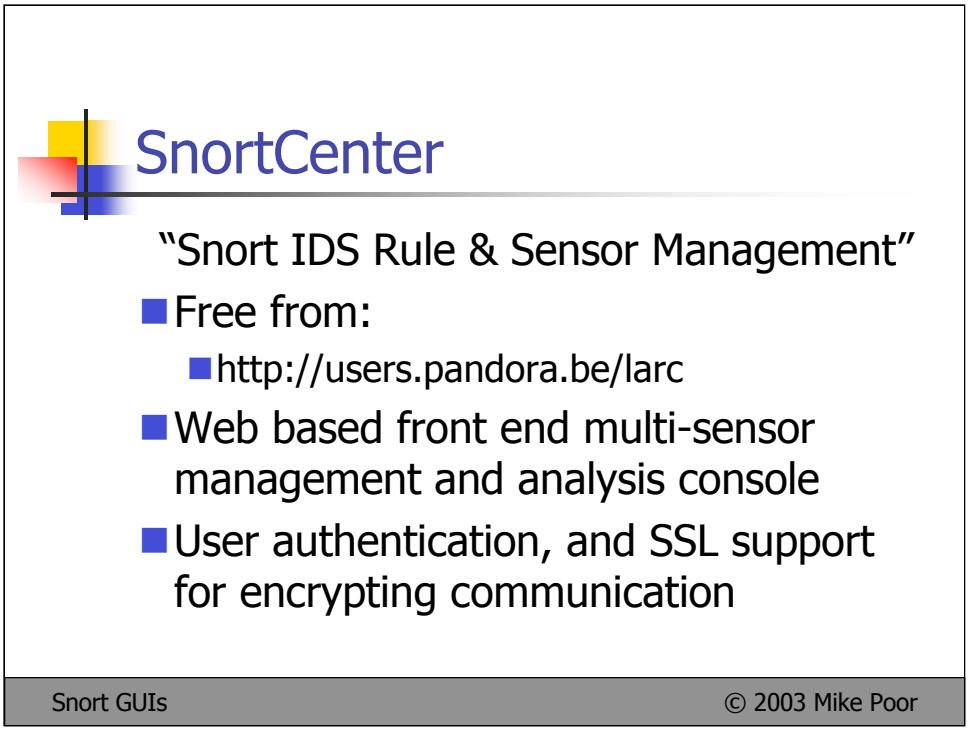
Acid Alert munging



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

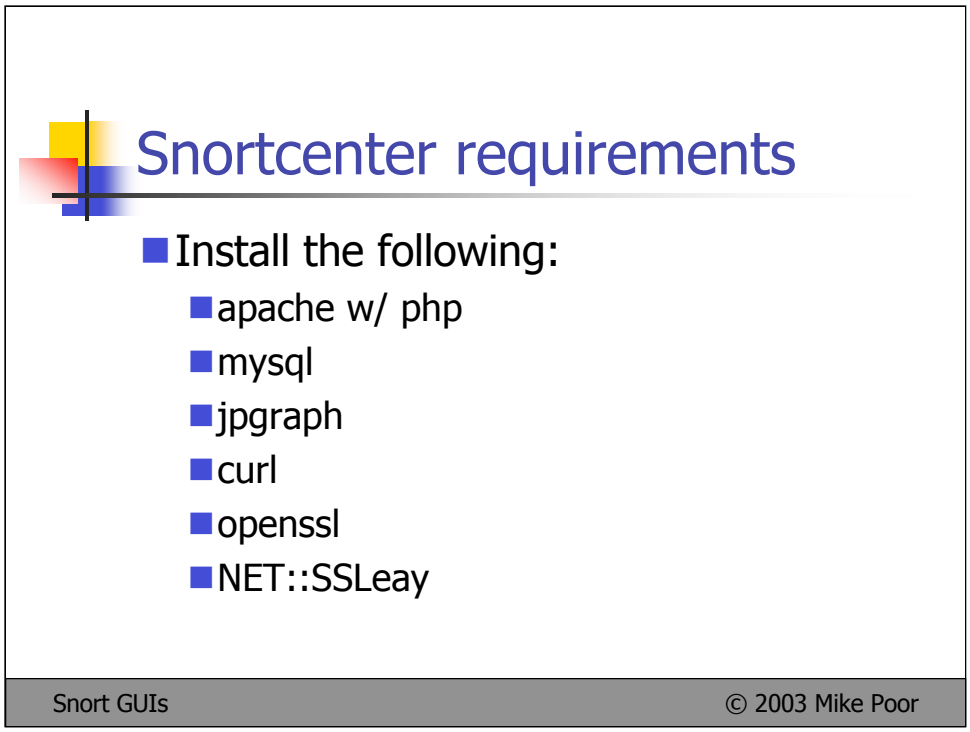
Acid Pros and Cons

Pros	Cons
■ Free, GPL	■ Slow
■ Well documented	■ resource intensive
■ Full web based front end for snort	■ Heavy maintanance
■ Designed for analysis	■ Does not scale to the enterprise level
	■ limited operation on events



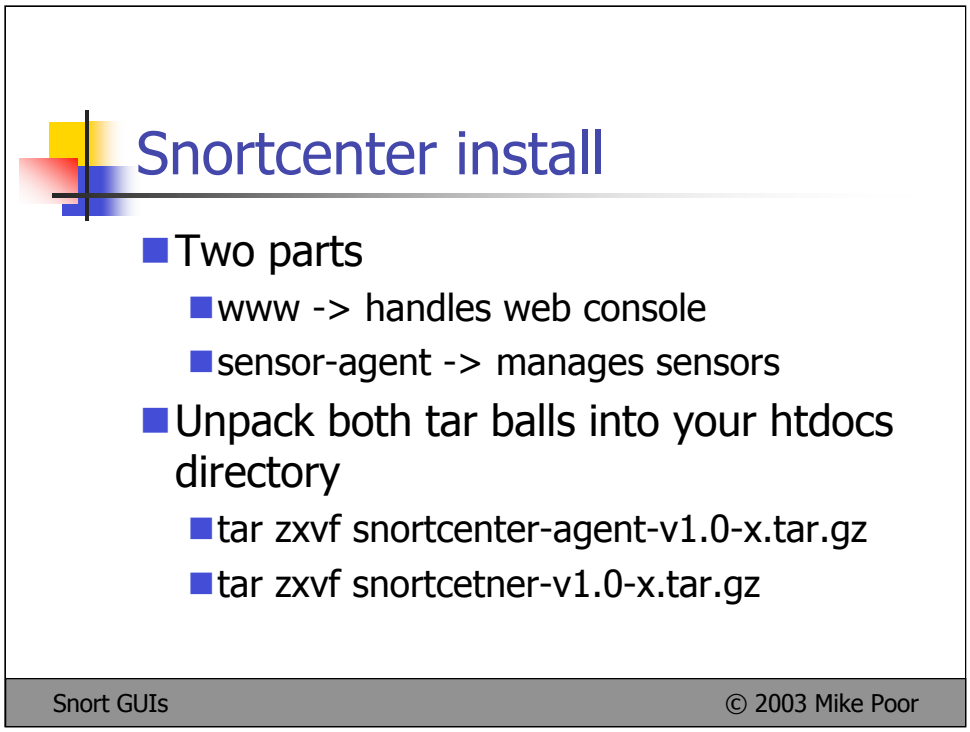
http://users.pandora.be/larc/

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

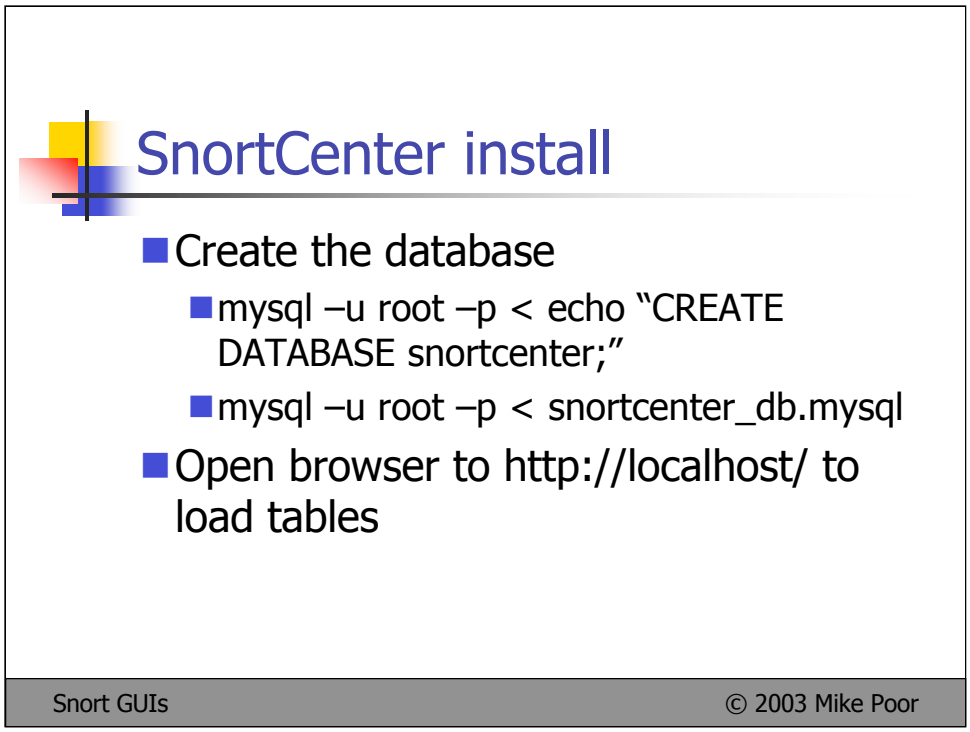


from http://users.pandora.be/larc :

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/



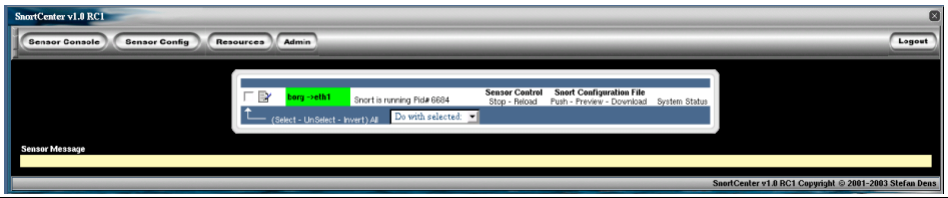
The install comes with two parts. A web console section, and a sensor management section. If you are installing both parts on one machine, untar the packages in your htdocs directory of your webserver.



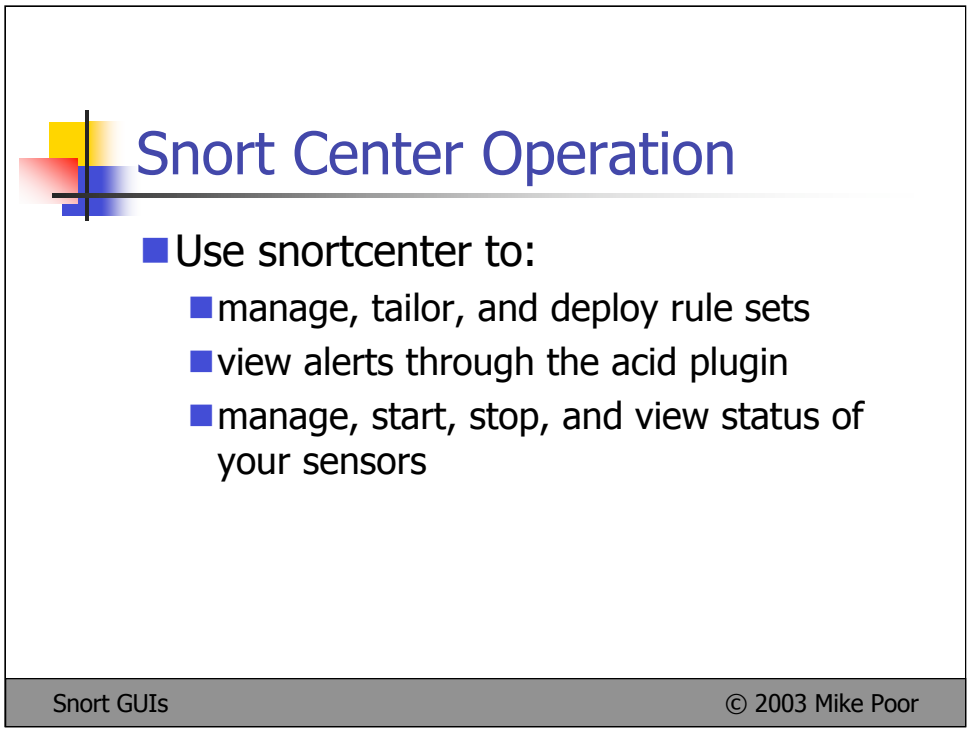
Follow directions in INSTALL file for database installation.

SnortCenter Install

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



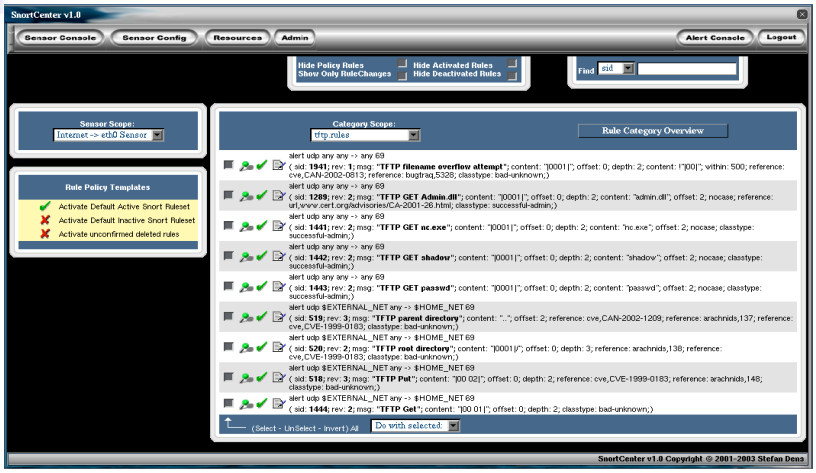
Now that you have configured your web console, its time to configure your sensor. The sensor can be added from http://localhost/ by clicking on <Sensor Console><Add Sensor>



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

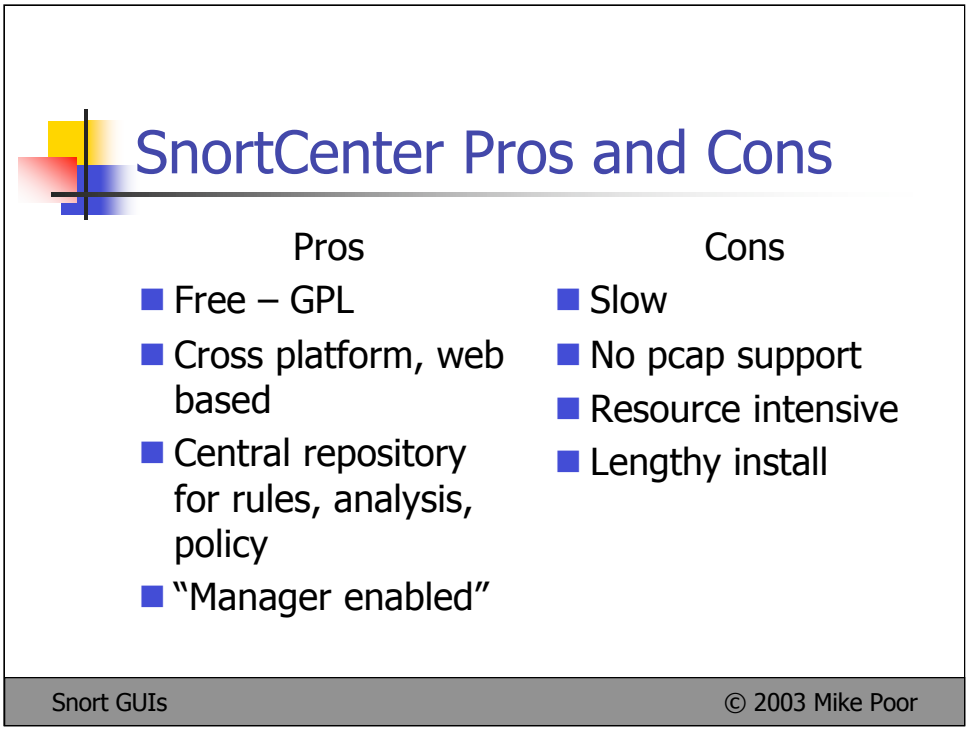
http://users.pandora.be/larc/documentation/snort_enterprise.pdf

Rule management

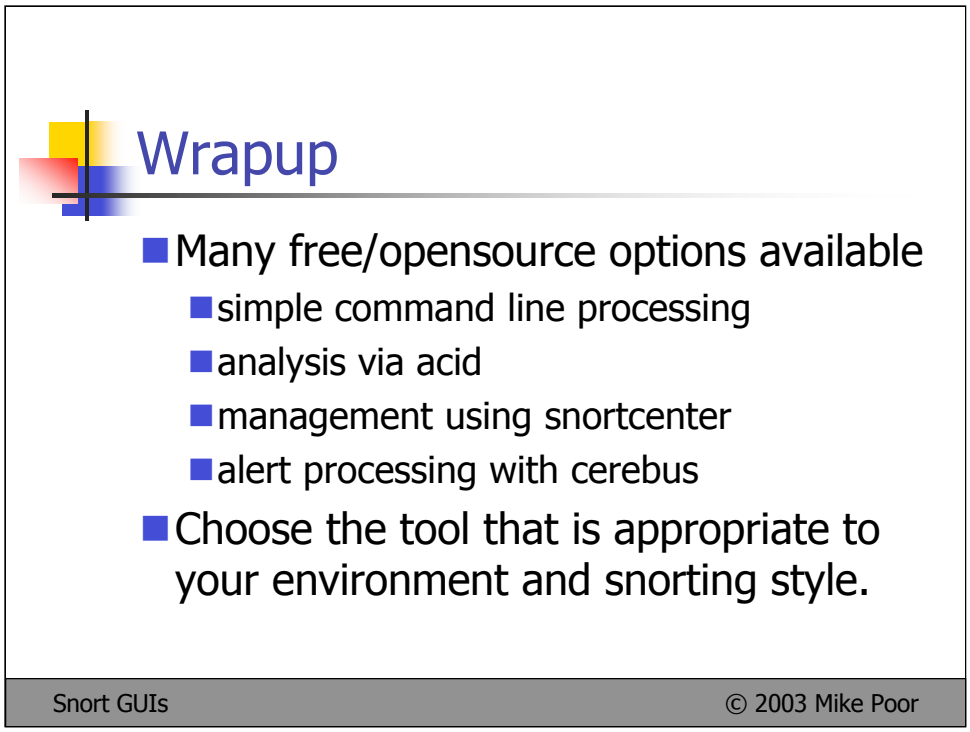


Rules template creation. Screenshot courtesy SnortCenter.

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



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



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.