Snort® Installation, Configuration and Basic Usage

Ed Mendez
Director, Instructional Design & Development

SOURCEfire

Overview:

- Planning a deployment
- Preparing the installation platform
- Software requirements
- Performing the installation
- Basic Snort operations
- Tuning strategies
- Q&A

Planning A Deployment

- Inline vs. Passive
  - How will your sensor fit into your existing architecture?
    - Switch span ports
    - Taps
  - Visibility to the assets you wish to protect
- Stand-alone sensors vs. distributed architectures
  - Visibility between the devices you need to communicate with
  - Access controls

Preparing The Installation Platform

- Hardware Considerations
  - Memory vs. CPU
  - Interfaces
    - Inline
    - Passive
  - Other hardware considerations
    - Disks
    - Motherboard bus architecture
- OS choice & preparation
  - Harden the platform

Software Requirements

- Software
  - Install from source or …
  - Install from pre-built binary package (RPM, Debian, etc.)
    - For packages, use a package management tool like Yum or apt-get
- Database, Web Server & PHP
  - The most popular choices are MySQL and Apache
  - Include the mysql, mysql-devel and mysql-server packages for your installation
  - For PHP, also include the php, php-gd, php-mysql, php-devel & php-pear packages

Software Requirements

- Snort requisite software:
  - Snort engine – preferably, the most current release
  - Snort rules – register or subscribe
  - Libpcap
  - PCRE
  - Libnet-1.0.2.a
  - Unified output processing tool (Barnyard)
- Other tools:
  - BASE
  - ADODB

Performing The Installation

Inline or Passive?

- For inline, make sure you choose the `--enable-inline` compile-time flag
- Choose the compile-time flags that enable the features you want in the binary you produce
- Do a `./configure –h` to get a listing of the available options
- Some common options are as follows:

```
--with-mysql
--enable-flexresp
--enable-perfprofiling
```

Performing The Installation

Preliminary Configuration:

- Make directories for the following:
  - For rules and configuration files
    - For example: `/etc/snort` & `/etc/snort/rules`
  - For Snort logging
    - For example: `/var/log/snort`
- Unpack your rules into the rules directory
- Copy configuration files from the location where you unpacked the Snort archive to the directory you created for storing configuration files
- Create a symbolic link of the Snort binary to the `/usr/sbin/snort` directory
- Create a user and group to run Snort and assign ownership of the Snort logging directory to this user and group
- Edit the `snort.conf` file to point to the correct location of your rules and enable database output

Performing The Installation

Preliminary Configuration:

- Setting up the database in the MySQL client
  - Set passwords for the users that will access the database. For example:
    - For the `root` user

```
set password for root@localhost=password(‘password’);
```

    - For the `snort` user

```
set password for snort@localhost=password(‘password’);
```

  - Create the alert database

```
create database snort;
```

  - Grant usage rights to the `snort` user

```
grant create, insert, select, delete, update on snort.*
  to snort@localhost;
```

Performing The Installation

- Preliminary Configuration:
  - Setting up the database schema
    - Check the schemas directory under the location where you unpacked the Snort archive for the schema that corresponds to the database platform you are using
    - For MySQL, you would issue the following command:

```
mysql -p < create_mysql snort
```

(you will be prompted for the password you issued in the previous slide)

Performing The Installation

Preliminary Configuration:

- Start Snort and test

```
snort -c /etc/snort/snort.conf
```

- Set the ownership and permissions for the Snort user in the logging directory

```
chown snort:snort /var/log/snort
chmod 600 /var/log/snort/alert
```

Performing The Installation

- Preliminary Configuration:
  - Setting up the graphical interface
    - Identify the root of your web server's directory structure
    - Unpack the BASE and ADODB packages into that directory
    - Edit the error reporting option in `php.ini` to read as follows:

```
error_reporting = E_ALL & ~E_NOTICE
```

    - Restart the HTTPD service

Performing The Installation

Configure the Snort startup

- The Snort tarball ships with a startup and startup configuration script located in the `rpm` directory
- Copy these files to the appropriate directories as follows:

```
cp /usr/local/snort-2.8.0.1/rpm/snortd /etc/init.d
cp /usr/local/snort-2.8.0.1/rpm/snort.sysconfig
  /etc/sysconfig/snort
```

- Use sym-links to link the `snortd` file to properly named start and kill scripts in the run level directories you intend to use

  Start format – `S##snortd`

  Kill format – `K##snortd`

Performing The Installation

- Tune the Snort startup configuration
  - The startup configuration is controlled via the file you just copied into the `/etc/sysconfig` directory
  - Edit the following areas of this file
    - Interface – set this to the interface you wish to sniff on
    - Alertmode – set to fast by default, you can comment this out
    - Binary_log – turned on by default. Comment this out to control how your logging takes place in the `snort.conf` file

Basic Snort Operations

- Snort can run in either of the following modes:
  - Packet sniffer
  - Packet logger
  - IDS/IPS
- For simple sniffing, do the following:
  - `snort -dev`
- For logging packets, specify an output directory (-l) and, optionally, a file name prefix (-L)

```
snort -dev -l /var/log/snortdump -L snort.output
```

  - Add a BPF for more specific output

Basic Snort Operations

Reading PCAP data with Snort

- Use the –r switch

```
snort -r snort.output.1082135914 -dev
```

- Add a BPF for more specific output

```
snort -r snort.output.1082135914 -dev
  src host 192.168.1.10
```

Basic Snort Operations

- Running Snort as an IDS
  - Start Snort with a configuration file

```
snort -c /etc/snort/snort.conf
```

- Running Snort as an IPS
  - Start Snort with a configuration file and the –Q switch to pick up network traffic from ip_queue and the –i switch to specify the bridged interface set

```
snort -Q -i br0 -c /etc/snort/snort.conf
```

Tuning Strategies

- Only enable rules needed to protect your environment
- Configure preprocessors for your environment; default settings can trigger false alerts
- Tune the variables in `snort.conf`
- Be careful when writing custom rules
  - Poorly crafted rules can have the following implications:
    - Performance impact
    - Prone to false positives
    - Potentially produce false negative situations

Education Offerings

- **Snort I and II Instructor-led Training (4-days)**
  - Installation, configuration, operation, output processing, rule management, tuning preprocessors, rule turning, using advanced rule options
  - Distributed Snort Installation, database management Snort in-line, using high-performance packet capture drivers, creating high-precision rules with the flowbits rule option.

- **SnortCP (Certified Professional) Certification Exam**

  60-Day Subscription, 2 Attempts, 200 Questions, 4 Hours, Score 75% >

- For pricing or other information contact training@sourcefire.com or call 734.743.6550 or 866.505.9113.

Thank you for attending!

Use promotion code SNORT27208 receive a 10% discount

Valid for next 30 days or until March 31, 2008

(not valid with any other discounts or offerings)

SOURCEfire

Security for the real world.

Sourcefire Commercial Products

- **Sourcefire 3D™ System**
- Sourcefire 3D Sensors
  - Sourcefire IPS™
  - Sourcefire RNA™
  - Sourcefire RUA™
  - Sourcefire NetFlow Analysis
- Sourcefire Defense Center™
- Sourcefire Intrusion Agent for Snort

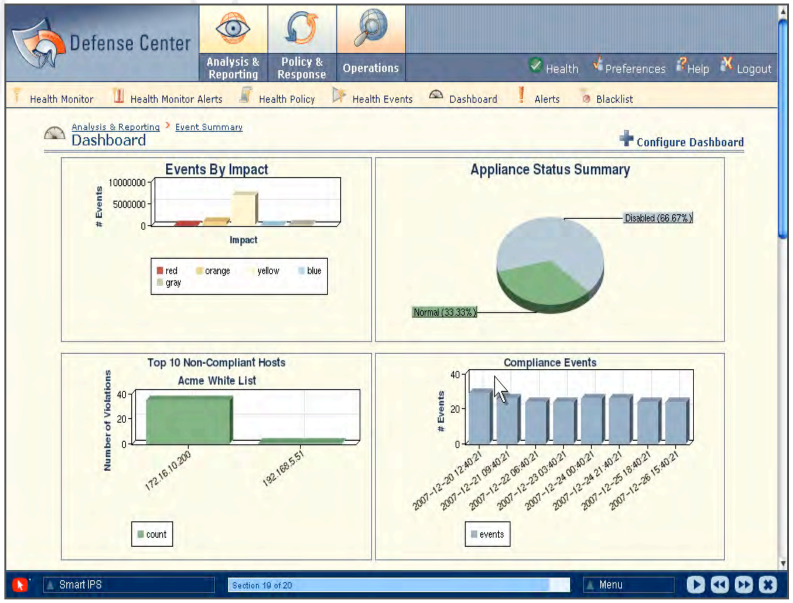
SOURCEfire
Security for the real world.

Why Upgrade to the 3D System?

- Purpose-built appliances
- World-class technical support
- Centralized event aggregation and analysis
- Reduce actionable events by 99% or more
- Automated IPS tuning
- Create custom reports and alerts
- Establish and monitor IT policy compliance
- Real-time, 24x7 passive network intelligence

For More Information…

Sourcefire 3D System Flash Demo



"Extending Your Investment in Snort" Technology Brief

SOURCEfire
Security for the real world

TECHNOLOGYBRIEF

Extending Your Investment in SNORT®

Discover. Determine. Defend.

Available Now on Sourcefire.com

Questions?

Please submit questions via the Q&A interface in the lower-right corner of your screen.