Snort

From the project **home page (http://www.snort.org/)**:

> Snort® is an open source network intrusion prevention and detection system (**IDS**/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

Contents

- 1 General Setup and Notes
- 2 Installation
- 3 Configuration
  - 3.1 Inline mode
  - 3.2 IDS mode
- 4 Updating the rules with Pulledpork
  - 4.1 Configuration
  - 4.2 Drop traffic with Pulledpork

  - 4.3 Disabling rules with Pulledpork
  - 4.4 Running Pulledpork
- 5 Update the rules: Oinkmaster
  - 5.1 Oinkmaster setup
  - 5.2 Oinkmaster usage
- 6 See also

General Setup and Notes

- A Snort setup that sniffs WAN <-> LAN is more difficult to use. It does not show you which computer triggered the alert, and it requires you to set HOME_NET as your WAN IP address, which can change if your modem uses DHCP.
- Snort will bridge the two interfaces for you, you will not need to configure this.

You can use Snort to sniff wireless traffic with two routers. For simplicity the router with *DHCP on and wireless off* will be called "router A" and the router with *wireless on and DHCP off* "router B".

- Ensure the routers do not have the same IP address, but are on the same subnet.
- If the machine running Snort is configured for inline mode, you will need 3 network interface cards. One for management, one for incoming traffic, and one for outgoing traffic.
- Connect a ethernet cord from router B to a spare NIC on the Snort machine.

- Connect another ethernet cord from router A to a spare NIC on the Snort machine.
- Once Snort is running traffic should flow from router B <-> Snort machine <-> router A <-> internet.
- If you are not using inline mode, then the traffic will need to be forwarded to the Snort machine, see: **Port Mirroring**

Installation

Install `snort (https://aur.archlinux.org/packages/snort/)`AUR from the **AUR**.

Configuration

The main configuration file is located at `/etc/snort/snort.conf`.

Let Snort know what network (or networks) you want to monitor.

```
ipvar HOME_NET [10.8.0.0/24,192.168.1.0/24]
```

At the bottom of the file, there is a list of includes. If you are going to use Pulledpork to download your rule set, then comment out all of the includes except for:

```
include $RULE_PATH/snort.rules
```

Inline mode

Inline mode means that packets pass *through* snort, rather than being diverted to snort. In this mode, snort can drop packets and abort exploitation attempts in real-time. In this mode, snort acts as an intrusion prevention system (IPS).

If you are planning on using Snort in inline mode add these lines to the bottom of the configuration:

```
config policy_mode:inline
config daq: afpacket
config daq_mode: inline
config daq_var:  buffer_size_mb=1024
```

A working example of inline mode in `snort.conf` is also available on **pastebin (http://pastebin.com/xNuVtni3)**.

Then ensure your service file `/usr/lib/systemd/system/snort@.service` has the correct arguments for inline mode. This meant adding `-Q` to the service file. Also Snort advises you to turn off LRO and GRO, **source (http://manual.snort.org/node7.html)**.

```
[Unit]
Description=Snort IDS system listening on '%I'

[Service]
Type=simple
ExecStartPre=/usr/sbin/ip link set up dev %I
ExecStartPre=/usr/bin/ethtool -K %I gro off
ExecStart=/usr/bin/snort --daq-dir /usr/lib/daq/ -A fast -b -p -u snort -g snort -c /etc/snort/snort.conf -i %I -Q
```

```
[Install]
Alias=multi-user.target.wants/snort@%i.service
```

To start Snort that is configured for inline mode run (*your network interfaces may vary*):

```
systemctl start snort@ens1:ens4
```

IDS mode

In intrusion detection mode (IDS), packets are diverted to snort. Snort can not drop packets, which means that it can only notify you that a exploitation attempt is occuring, or have already occured.

To start Snort in IDS mode run:

```
systemctl start snort@ens1
```

Updating the rules with Pulledpork

Install **pulledpork (https://aur.archlinux.org/packages/pulledpork/)**AUR from the **AUR**.

Configuration

The configuration files are located in `/etc/pulledpork`

Edit `/etc/pulledpork/pulledpork.conf` and uncomment the rules you want to use. You will need an "oinkcode" to download some of the rules.

- `dropsid.conf` any rules matched in this file will have its traffic dropped.
- `enablesid.conf` is used to enable signatures. All signatures seem to be enabled by default, no need to edit this file.
- `disablesid.conf` is used to completely remove a signature from Snort.

The current categories that are within your rule set can be found by running the following:

```
pulledpork.pl -c /etc/snort/pulledpork.conf -Pw
lz /var/tmp/*.gz | egrep '\.rules' | cut -d'/' -f3 | sort -u | perl -lne '/(.*).rules/ && print $1' > rules.`date +%F`
```

Drop traffic with Pulledpork

If you want to drop *all* traffic that matches a Snort signature instead of just alerting, add the following to your `dropsid.conf`:

```
pcre:.
```

Or if you want to drop all traffic matching an entire category:

```
policy-social
policy-other
file-other
```

If you only want to drop a single rule:

```
118:7
```

Disabling rules with Pulledpork

If you want to disable a single signature add its gen_id and sig_id to `/etc/pulledpork/disablesid.conf`

```
118:22
```

If you want to disable an entire category:

```
deleted
protocol-icmp
policy-social
policy-other
```

Running Pulledpork

This will pull the new rules and write them to `/etc/snort/rules/snort.rules`

```
pulledpork.pl -c /etc/pulledpork/pulledpork.conf  -P
```

Update the rules: Oinkmaster

If you want to be able to download Snort's latest rules, you will need a subscription. This costs money. If you are happy enough with 5 days old rules, you just need to register for free. If you do not, the only updates you will get are the new rules distributed with a new Snort release. Go ahead and register at **Snort (https://www.snort.org/signup)**. If you really do not want to register, you can use the rules from **BleedingSnort.com (http://www.bleedingsnort.com/)**. They are bleeding edge, meaning they have not been tested thoroughly.

`oinkmaster (https://aur.archlinux.org/packages/oinkmaster/)`AUR is available as **AUR** package.

Oinkmaster setup

Edit `/etc/oinkmaster.conf` and look for the URL section and uncomment the 2.4 line. Make sure to replace <*oinkcode*> by the Oink code you generated after logging into your Snort account. For Bleeding Snort rules, uncomment the appropriate line.

When you log into your new account, create an "Oink code". Another thing to change is

```
use_external_bins=1 # 1 uses wget, tar, gzip instead of Perl modules
```

The rest of the configuration file is fine.

Oinkmaster usage

```
oinkmaster.pl -o /etc/snort/rules
```

Create an executable script with the exact command and place it in /etc/cron.daily to update the rules daily automatically.

See also

- **Simple stateful firewall**
- **Router**

Retrieved from "https://wiki.archlinux.org/index.php?title=Snort&oldid=508645"

- This page was last edited on 27 January 2018, at 12:59.
-