Suricata

From the project **home page (http://suricata-ids.org/)**:

> Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

Contents

Installation

Install `suricata (https://aur.archlinux.org/packages/suricata/)`[AUR] from the AUR.

Configuration

The main configuration file is `/etc/suricata/suricata.yaml`.

You should change the following parts of the config in order to make it run:

```
default-log-dir: /var/log/suricata/     # where you want to store log files
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
HOME_NET: "[10.0.0.0/8]"                # your local network
host-os-policy:   ..                    # according to the OS running the ips
magic-file: /usr/share/file/misc/magic.mgc
```

Web interface

You may use snorby [1] (https://github.com/Snorby/snorby) as web interface.

Starting Suricata

Manual startup

You may start the suricata service manually with:

```
# /usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth0
```

Systemd service configuration

To start suricata automatically at system boot, **enable** `suricata@<interface>.service`.

For example, if the network interface is `eth0`, the service name is `suricata@eth0.service`.

Tip: If the service file is not yet included in AUR you can find it here: **[2] (http://archlinux.pastebin.com/RAtGPVL9)**. Place this file under `/usr/lib/systemd/system/suricata@.service`

Retrieved from "https://wiki.archlinux.org/index.php?title=Suricata&oldid=508647"
