Suricata Intrusion Detection System

Install dan konfigurasi

```
sudo apt-get install suricata
sudo vim /etc/default/suricata
```

Ubah RUN=no menjadi RUN=yes :

```
:%s/RUN=no/RUN=yes/
```

Simpan, lalu keluar dengan `:wq [enter]`. Edit juga berkas konfigurasinya :

```
sudo vim /etc/suricata/suricata-debian.yaml
```

Sesuaikan konfigurasi, lalu restart suricata :

```
sudo service suricata restart
```

Hampir nyerah, akhirnya ketika paket tersebut akan saya hapus, muncul pesan error :

```
samsul@studio-server~$ sudo apt-get purge suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  libcap-ng0 libhtp1 libjansson4 libluajit-5.1-2 libluajit-5.1-common
libmnl0
  libnet1 libnetfilter-queue1 libnspr4 libnss3 libnss3-nssdb libprelude2
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  suricata*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
1 not fully installed or removed.
After this operation, 2140 kB disk space will be freed.
Do you want to continue? [Y/n] y
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
    LANGUAGE = (unset),
    LC_ALL = (unset),
    LC_TIME = "id_ID.UTF-8",
    LC_MONETARY = "id_ID.UTF-8",
    LC_ADDRESS = "id_ID.UTF-8",
    LC_TELEPHONE = "id_ID.UTF-8",
    LC_NAME = "id_ID.UTF-8",
    LC_MEASUREMENT = "id_ID.UTF-8",
    LC_IDENTIFICATION = "id_ID.UTF-8",
```

```
    LC_NUMERIC = "id_ID.UTF-8",
    LC_PAPER = "id_ID.UTF-8",
    LANG = "id_ID.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
locale: Cannot set LC_CTYPE to default locale: No such file or directory
locale: Cannot set LC_MESSAGES to default locale: No such file or directory
locale: Cannot set LC_ALL to default locale: No such file or directory
(Reading database ... 96569 files and directories currently installed.)
Removing suricata (1.4.7-1ubuntu1.1) ...
 * NFQUEUE support not found !
 * Please ensure the nfnetlink_queue module is loaded or built in kernel
invoke-rc.d: initscript suricata, action "stop" failed.
dpkg: error processing package suricata (--purge):
 subprocess installed pre-removal script returned error exit status 5
 * NFQUEUE support not found !
 * Please ensure the nfnetlink_queue module is loaded or built in kernel
invoke-rc.d: initscript suricata, action "start" failed.
dpkg: error while cleaning up:
 subprocess installed post-installation script returned error exit status 5
Errors were encountered while processing:
 suricata
E: Sub-process /usr/bin/dpkg returned an error code (1)
```

Masih error juga? Edit kembali berkas `/etc/default/suricata`, lalu ubah:

```
:%s/LISTENMODE=nfqueue/LISTENMODE=pcap/
```

Ubah juga interface yang digunakan. Simpan, lalu restart kembali suricata.

<wrap em>Tulisan ini hanya sebagai catatan pribadi saja, tidak diperuntukkan untuk mesin produksi. Jika Anda mengikuti panduan ini, lalu sistem Anda mengalami masalah, silahkan ditanggung sendiri.</wrap>

Referensi

- http://blog.mattbrock.co.uk/hardening-the-security-on-ubuntu-server-14-04/
- http://community.plusonnet.co.kr/?p=1169
- https://bugs.launchpad.net/ubuntu/+source/suricata/+bug/1250439