Ubuntu Installation

Pre-installation requirements

Before you can build Suricata for your system, run the following command to ensure that you have everything you need for the installation.

```
sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \
build-essential autoconf automake libtool libpcap-dev libnet1-dev \
libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 \
make libmagic-dev
```

Depending on the current status of your system, it may take a while to complete this process.

HTP
HTP is bundled with Suricata and installed automatically. If you need to install HTP manually for other reasons, instructions can be found at HTP library installation.

IPS
By default, Suricata works as an IDS. If you want to use it as a IDS and IPS program, enter:

```
sudo apt-get -y install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0
```

Suricata

To download and build Suricata, enter the following:

```
wget http://www.openinfosecfoundation.org/download/suricata-1.4.4.tar.gz
tar -xvzf suricata-1.4.4.tar.gz
cd suricata-1.4.4
```

Compile and install the engine

If you plan to build Suricata with IPS capabilities, enter:

```
./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

instead of

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

Continue with the next commands:

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
make
sudo make install
sudo ldconfig
```

Auto setup

You can also use the available auto setup features of Suricata:

ex:

> *./configure && make && make install-conf*

make install-conf
would do the regular "make install" and then it would automatically create/setup all the necessary directories and suricata.yaml for you.

> *./configure && make && make install-rules*

make install-rules
would do the regular "make install" and then it would automatically download and set up the latest ruleset from Emerging Threats available for Suricata

> *./configure && make && make install-full*

make install-full
would combine everything mentioned above (install-conf and install-rules) - and will present you with a ready to run (configured and set up) Suricata

Please continue with Basic Setup.

ubuntu_logo.jpg (7.68 KB) Anne-Fleur Koolstra, 03/22/2011 06:01 am