CENTOS 6 Getting Started with Suricata

INTRO:

This is a guide to install Suricata with PF_RING. This installation was completed using Virtualbox version 4.0.6 and CentOS 6.0-i386.

Sections:

1. Basic Suricata installation and how to enable some features
2. PF_RING (capture accelerator) Suricata installation with features from Section 1
3. Suricata Configuration

Required Packages To Build Suricata:

```
sudo yum -y install libpcap libpcap-devel libnet libnet-devel pcre

pcre-devel gcc gcc-c++ automake autoconf libtool make libyaml

libyaml-devel zlib zlib-devel
```

Install Suricata as and IDS and IPS system

Xi386

```
sudo rpm -Uvh
http://rules.emergingthreatspro.com/projects/emergingrepo/i386/libnetfilter_q
ueue-0.0.15-1.i386.rpm \

http://rules.emergingthreatspro.com/projects/emergingrepo/i386/libnetfilter_q
ueue-devel-0.0.15-1.i386.rpm \

http://rules.emergingthreatspro.com/projects/emergingrepo/i386/libnfnetlink-
0.0.30-1.i386.rpm \

http://rules.emergingthreatspro.com/projects/emergingrepo/i386/libnfnetlink-
devel-0.0.30-1.i386.rpm
```

X86_64:

```
sudo rpm -Uvh
http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter
_queue-0.0.15-1.x86_64.rpm \

http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnetfilter
_queue-devel-0.0.15-1.x86_64.rpm \

http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink
-0.0.30-1.x86_64.rpm \
```

```
http://rules.emergingthreatspro.com/projects/emergingrepo/x86_64/libnfnetlink
-devel-0.0.30-1.x86_64.rpm

# cd /opt

# wget http://www.openinfosecfoundation.org/download/suricata-1.0.5.tar.gz

# tar -xvfz suricata-1.0.5.tar.gz

# cd suricata-1.0.5

#sudo ./configure  --enable-nfqueue

#sudo make

#sudo make install
```

To install enable additional features of Suricata , install the following packages and append the ./configure line as stated:

To Enable HTP Library(HTML pre-processor) feature:

```
#wget http://www.openinfosecfoundation.org/download/libhtp-0.2.3.tar.gz

#tar -xzvf libhtp-0.2.3.tar.gz

#cd libhtp-0.2.3

#./configure

#make

#make install
```

To enable libcap_ng (dropping privileges) feature:

```
#wget http://people.redhat.com/sgrubb/libcap-ng/libcap-ng-0.6.4.tar.gz
#tar -xzvf libcap-ng-0.6.4.tar.gz
#cd libcap-ng-0.6.4
#./configure
#make
#sudo make install
```

2.PF_RING installation

This installation will install PF_RING as well as enable the above features.

2.1 Download the required packages:

```
#apt-get install build-essential libpcre3-dev libpcap-dev libnet1-dev
libyamldev libnetfilter-queue-dev zlib1g-dev htp subversion flex bison
kernel-devel dkms nano
```

Note Please you will need to download the correct kernel headers for your specific system

2.2 Download PF_RING

```
# cd /usr/src

# svn --force export https://svn.ntop.org/svn/ntop/trunk/PF_RING/
PF_RING_CURRENT_SVN

# mkdir /usr/src/pf_ring-4

# cp -Rf /usr/src/PF_RING_CURRENT_SVN/kernel/* /usr/src/pf_ring-4/
```

2.3 Configure PF_RING Driver

```
# cd /usr/src/pf_ring-4/

# nano dkms.conf
```

PACKAGE_NAME="pf_ring"
PACKAGE_VERSION="4"
BUILT_MODULE_NAME[0]="pf_ring"
DEST_MODULE_LOCATION[0]="/kernel/net/pf_ring/"
AUTOINSTALL="yes"

Then press CRTL+X, Y, Enter

```
# dkms add -m pf_ring -v 4

# dkms build -m pf_ring -v 4 –kernelsourcedir /usr/src/kernels/(Insert kernel
header)

# dkms install -m pf_ring -v 4
```

At the end the install command you should get DKMS: INSTALL Completed

NOTE To remove the pf_ring driver type the following command:

```
#sudo dkms remove –m pf_ring –v 4  --all
```

2.4 Install PF_RING

```
#sudo cp -f /usr/src/PF_RING_CURRENT_SVN/kernel/linux/pf_ring.h
/opt/PF_RING/include/linux/

#cd /usr/src/PF_RING_CURRENT_SVN/userland/lib

#sudo ./configure  --prefix=/opt/PF_RING/

#sudo cp -f pfring_e1000e_dna.h /opt/PF_RING/include
```

```
#sudo make

#sudo make install
```

3. Download and configure Suricata with pf_ring

3.1 A Stable version:

```
# cd /opt

# wget http://www.openinfosecfoundation.org/download/suricata-1.0.5.tar.gz

# tar xvfz suricata-1.0.5.tar.gz

# cd suricata-1.0.5

#Sudo ./configure --enable-pfring --with-libpfring-libraries=/opt/PF_RING/lib
--with-libpfring-includes=/opt/PF_RING/include                              --
with-libpcaplibraries=/opt/PF_RING/lib                                          -
-with-libpcap-includes=/opt/PF_RING/include
LD_RUN_PATH="/opt/PF_RING/lib:/usr/lib:/usr/local/lib"                 --
prefix=/opt/PF_RING/

# sudo  make

# sudo make install
```

3.2 Configure Suricata

```
#mkdir  /etc/suricata

#mkdir  /var/log/suricata
```

3.2A Stable Version:

```
#sudo cp /opt/suricata/suricata.yaml classification.conf /etc/suricata
```

3.3 Adding Rules to Suricata

See Suricata Wiki:

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Rule_Management_with_Oinkmaster

3.4.Run Suricata:

```
#sudo /opt/PF_RING/bin/suricata  –c  /etc/suricata/suricata.yaml –i eth0
```