HOWTO-Suricata IDS on Debian 5.0 (Lenny)

Miguel Angel Cabrerizo, doncicuto@gmail.com

v0.2, 8 July 2010

This is a howto for installing Suricata IDS on Debian 5.0. This howto will explain how to install and configure Suricata as IDS or IPS. At the time of this writing only installation is covered. This howto uses Stein Gjoen's template for small HOWTOs (http://www.nyx.net/~sgjoen/mintplt.html)

1. Introduction

On July 1, 2010 the *Open Information Security Foundation* released the first stable version of Suricata IDS. I'm a long time Snort user but I want to know more about this IDS so that´s why I'm writing this howto for Debian 5.0 (Lenny).

Suricata is ready for using PF_RING the new network socket that, according to *ntop's web* (what a great tool ntop is...), dramatically improves the packet capture speed.

Suricata installation is not difficult but it needs a little time if you want to use PF_RING. This howto uses the INSTALL and INSTALL.PF_RING files that comes with Suricata but with some modifications on my own.

The latest version of this document can be found at diatel.wordpress.com. I hope this document helps you in using Suricata.

1.1 Copyright

1.2 Disclaimer

Use the information in this document at your own risk. I disavow any potential liability for the contents of this document. Use of the concepts, examples, and/or other content of this document is entirely at your own risk.

All copyrights are owned by their owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.3 Credits

In this version I have the pleasure of acknowledging

```
     Victor Julien and William Metcalf
     Stein Gjoen
```

Any comments or suggestions can be mailed to my mail address on Gmail: doncicuto [at] gmail.com

2. Installation

2.1 Installing the prerequisites

After a fresh installation of Debian 5.0 (Lenny) you will need to download the following packages and install them. Change the linux headers package according to your server's configuration.

```
# apt-get install build-essential libpcre3-dev libpcap-dev libnet1-dev libyaml-
dev libnetfilter-queue-dev zlib1g-dev htp subversion flex bison linux-headers-
2.6.26-2-686
```

We'll need more packages from backports.org so edit your /etc/apt/sources.list:

```
# vi /etc/apt/sources.list
```

Add the new source and save the file:

```
deb http://www.backports.org/debian lenny-backports main contrib non-free
```

Update your package list

```
# apt-get update
```

If you find an error about the GPG keys please download the backports keyring and confirm the authenticity.

```
# apt-get install debian-backports-keyring
```

Update again your package list

```
# apt-get update
```

Install the following packages from backports.org

```
# apt-get -t lenny-backports install dkms libcap-ng-dev
```

2.2 Configure PF_RING

This is the toughest part, there are many steps so try not to get lost

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

Create a file called dkms.conf and place the following into the file.

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

```
# dkms add -m pf_ring -v 4
# dkms build -m pf_ring -v 4
# dkms install -m pf_ring -v 4
# mkdir /usr/src/e1000e-pf_ring-1.0.15
# cp -Rf /usr/src/PF_RING_CURRENT_SVN/drivers/intel/e1000e-1.0.15/src/*
/usr/src/e1000e-pf_ring-1.0.15/
# cp -f /usr/src/PF_RING_CURRENT_SVN/kernel/linux/pf_ring.h /usr/src/e1000e-
pf_ring-1.0.15/
# cd /usr/src/e1000e-pf_ring-1.0.15/
# sed -i -e 's/\.\.\/\.\.\/\.\.\/\.\.\/kernel\/linux\/pf\_ring\.h/pf\_ring\.h/'
netdev.c
```

Create a file called dkms.conf and place the following into the file.

```
PACKAGE_NAME="e1000e-pf_ring"
PACKAGE_VERSION="1.0.15"
BUILT_MODULE_NAME[0]="e1000e"
DEST_MODULE_LOCATION[0]="/kernel/drivers/net/e1000e/"
AUTOINSTALL="yes"
```

```
# dkms add -m e1000e-pf_ring -v 1.0.15
# dkms build -m e1000e-pf_ring -v 1.0.15
# dkms install -m e1000e-pf_ring -v 1.0.15

# mkdir -p /opt/PF_RING/{bin,lib,include/linux,sbin}
# 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
# sed -i -e 's/INSTDIR   = \${DESTDIR}\/usr\/local/INSTDIR   = \$
{DESTDIR}\/opt\/PF_RING/' Makefile
# cp -f pfring_e1000e_dna.h /opt/PF_RING/include
# make &&  make install

# cd /usr/src/PF_RING_CURRENT_SVN/userland/libpcap-1.0.0-ring
# sed -i -e 's/\.\.\/lib\/libpfring\.a/\/opt\/PF_RING\/lib\/libpfring\.a/'
Makefile
# sed -i -e 's/\.\.\/lib\/libpfring\.a/\/opt\/PF_RING\/lib\/libpfring\.a/'
Makefile.in
# ./configure --prefix=/opt/PF_RING && make && make install

# cd /usr/src/PF_RING_CURRENT_SVN/userland/tcpdump-4.0.0
# sed -i -e 's/\.\.\/lib\/libpfring\.a/\/opt\/PF_RING\/lib\/libpfring\.a/'
Makefile.in
# sed -i -e 's/-I \.\.\/libpcap-1\.0\.0-ring/-I \/opt\/PF_RING\/include/'
Makefile.in
# sed -i -e 's/-L \.\.\/libpcap-1\.0\.0-ring\/-L /\/opt\/PF_RING\/lib\//'
Makefile.in
# ./configure LD_RUN_PATH="/opt/PF_RING/lib:/usr/lib:/usr/local/lib"
--prefix=/opt/PF_RING/ --enable-ipv6 && make && make install
```

2.3 Configuring and installing Suricata

I'm going to configure Suricata with the following features:

- --enable-pfring (better packet capture performance)
- --with_libpcap-libraries (libpcap ready for PFRING)
- --with_libcap_ng-libraries (for dropping privileges)
- --enable-nfqueue (IPS capabilities)
- --with-libhtp-libraries (HTP HTML pre-processor)

First download Suricata current release to a directory, in my case, /opt

```
# cd /opt
# wget http://www.openinfosecfoundation.org/download/suricata-1.0.0.tar.gz
# tar xvfz suricata-1.0.0.tar.gz
# cd suricata-1.0.0
#  ./configure --enable-pfring --with-libpfring-libraries=/opt/PF_RING/lib
--with-libpfring-includes=/opt/PF_RING/include --with-libpcap-
libraries=/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/
--enable-nfqueue --with-libcap_ng-libraries=/usr/lib –with-libhtp-libraries
# make
# make install
```

You're ready to configure Suricata.

3. Basic configuration

3.1 Suricata user

It is always advisable to create a user account, with no privileges, to run Suricata.

```
# groupadd suricata
# useradd -g suricata suricata -s /sbin/nologin
```

3.2 Directories

Create a directory to store your logs and give permissions to the suricata user.

```
# mkdir /var/log/suricata
# chown suricata:suricata /var/log/suricata
```

Now you will need to create a directory to store configuration files

```
# mkdir /etc/suricata
```

Finally create a directory to store the rules

```
# mkdir /etc/suricata/rules
```

3.3 Config files

Now it's time to move Suricata's config files to its directory

```
# cp /opt/suricata-1.0.0/suricata.yaml /etc/suricata/
# cp /opt/suricata-1.0.0/classification.config /etc/suricata/
```

It's always good to have a threshold.conf file in case you want to disable rules or set a threshold for alerts.

```
# touch /etc/suricata/threshold.config
```

Spend a few minutes reviewing the well-documented suricata.yaml file.

These are my suggestions:

- As we are not using Prelude in this how-to comment the lines for alert-prelude

```
# - alert-prelude:
#    enabled: no
#    profile: suricata
```

- Change the HOME_NET variable.
- Add your servers to the HTTP_SERVERS, SMTP_SERVERS....
- I find interesting that Suricata logs to a file

outputs:

```
- console:
     enabled: yes

- file:
     enabled: yes
     filename: /var/log/suricata.log
```

3.4 Rules

There's no fun if your IDS/IPS has no rules so let's get some.

Emerging Threats is an open source community project managed by Matt Jonkman which provides free Snort and Suricata signatures. Download the latest rules and move them to the rules directory. ET rules will offer you the highest level of compatibility with Suricata.

```
# cd /usr/src
# wget http://www.emergingthreats.net/rules/emerging.rules.tar.gz
# tar xvfz emerging.rules.tar.gz
# mv /usr/src/rules/*.rules /etc/suricata/rules/
```

Snort.org also offers Sourcefire VRT Certified Rules to registered users free of charge 30-days after the initial release to subscribers. Once you have registered an user you will be able to download the current ruleset file. Uncompress it and move the rules.

```
# tar xvfz snortrules-snapshot-2860.tar.gz
# mv /usr/src/rules/*.rules /etc/suricata/rules/
```

Suricata will try it best to parse Snort's rules but don´t panic if the console starts showing errors with some signatures. Suricata is strong and the engine will finally start! In my case and for testing purposes I 've disabled all the Snort rules.

3.5 Change ownership

Don´t forget to change the ownership

```
# chown -R suricata:suricata /etc/suricata/
```

It's time to run Suricata for the first time!