Installation de Snort sous Fedora

S.N.O.R.T. est un NIDS (Network Intrusion Détection System ou Système de Détection d'Intrusion Réseau). Comme ses initiales le suggèrent, un NIDS sert à détecter les tentatives d'intrusion, pour ce faire, il compare le trafic réseau à une base de données des attaques connues. Le cas échéant, il exécute une action prédéfinie, qui va de vous prévenir à verrouiller le réseau.

S.N.O.R.T. vous permettra donc basiquement, de détecter d'éventuels intrusions, de gérer vos logs et sniffer le réseau. Nous détaillerons ici, l'installation à partir des sources, bien que de nombreuses distributions soient livrées avec un paquetage snort.

Cette installation comprend en fait 2 grandes parties :

- l'installation de snort (logiciel de base avec toutes ses dépendances)
- l'installation de l'ACID ; l'interface graphique avec les bases mysql qui vous permettra de suivre plus convivialement les détections d'intrusion.

I – Installation de snort :

1.1 – Prérequis :

PCRE :
Sur http://www.snort.org/, téléchargez **pcre-6.4.tar.gz** ou la dernière version que vous trouverez.
$]# *tar –zxvf pcre-6.4.tar.gz*
$]# *cd pcre-6.4*
$]# *./configure*
$]# *make*
$]# *make check*
$]# *make install*

Libpcap (Si ce n'est pas déjà fait) :
Téléchargement possible sur plein de sites. Exemple : sur ftp://ftp.ee.lbl.gov/libpcap.tar.Z
$]# *tar –zxvf libpcap.tar.Z*
$]# *cd libpcap-0.4/*
$]# *./configure --prefix=/usr*
$]# *make*
$]# *make install*
$]# *mkdir /usr/include/pcap*
$]# *mkdir /usr/include/pcap/net*
$]# *cp *.h /usr/include/pcap/*
$]# *cp bpf/net/*.h /usr/include/pcap/net/*

$]# *vi Makefile*
Dans le fichier Makefile, repérez la section de **install-man** et remplacer **$(DESTDIR)$(MANDEST)/man3/pcap.3** par **/usr/share/man/man3/pcap.3**
$]# *make install-man*

1.2 - Installation de SNORT :

Downloadez la dernière version sur http://www.snort.org/
Exemple : http://www.snort.org/dl/current/snort-2.4.3.tar.gz
$]# *tar –zxvf snort-2.4.3.tar.gz*
$]# *cd snort-2.4.3*
$]# *./configure --prefix=/usr --with-libpcap-includes=/usr/include/pcap --with-libpcap-libraries=/usr/lib --with-mysql=/var/lib/mysql*
Pour avoir toutes les options de compil, ouvrez le fichier configure, et recherchez la section **Optional Packages**.
$]# *make*
$]# *make install*
$]# *mkdir /etc/snort*
$]# *mkdir /etc/snort/rules*
$]# *cp etc/* /etc/snort/*
$]# */usr/sbin/useradd snort –d /var/log/snort –s /sbin/nologin –c "Program SNORT"*
$]# *chown –R snort:snort /var/log/snort*
Downloadez les rules minimales sur http://www.snort.org. Il va vous falloir vous enregistrer d'abord, puis télécharger ensuite. A supposer que vous ayez téléchargé **snortrules-snapshot-2.4.tar.gz** :
$]# *tar –zxvf snortrules-snapshot-2.4.tar.gz*
$]# *cp –R snortrules-snapshot-2.4/rules /etc/snort/rules*

Snort est ainsi installé avec les configs par défaut.

Vous pouvez l'utilisez en mode sniffer comme la commande tcpdump :

$]# *snort –v*
$]# *snort –vde*
$]# *snort –dvi eth0*

Mais il est plus intéressant lorsqu'on l'utilise en mode NIDS, et pour cela des configs s'imposent.

1.3 - Configuration basique de snort

Toute la config se fait dans le fichier **/etc/snort/snort.conf** qui contient un certain nombre de variables à paramétrer et c'est tout.

Donc éditez le fichier et modifions le ensemble :
Les lignes commençant par # sont des commentaires, elles sont en fait remplacées par la ligne qui les suit :

Spécifier votre réseau que vous voulez surveiller :

```
# var HOME_NET any # Roger
var HOME_NET [196.200.10.0/24,196.200.72.176/28]
```

Spécifier les autres (la jungle) :

```
# Set up the external network addresses as well.  A good start may be "any"
# var EXTERNAL_NET any # Roger
var EXTERNAL_NET !$HOME_NET
```

Spécifier vos serveurs DNS :

```
# List of DNS servers on your network
# var DNS_SERVERS $HOME_NET # Roger
var DNS_SERVERS [196.200.12.6/32,196.200.12.130/32]
```

Indiquer vos serveurs de messagerie :

```
# List of SMTP servers on your network
# var SMTP_SERVERS $HOME_NET # Roger
var SMTP_SERVERS 196.200.17.130/32
```

Indiquer vos serveurs web :

```
# List of web servers on your network
# var HTTP_SERVERS $HOME_NET # Roger
var HTTP_SERVERS [196.200.18.132/32,207.251.21.231/32]
```

Indiquer le chemin des règles que vous avez téléchargées :

```
var RULE_PATH /etc/snort/rules
```

Un certain nombre de chinoiserie (je donne juste les parties que j'ai modifiées dans ma config) :

```
# preprocessor frag3_engine: policy first detect_anomalies  # Roger
preprocessor frag3_engine: policy first detect_anomalies bind_to 196.200.10.0/24

#preprocessor http_inspect_server: server default \
#    profile all ports { 80 8080 8180 } oversize_dir_length 500 # Roger
preprocessor http_inspect_server: server default \
   profile all ports { 80 } oversize_dir_length 500

#preprocessor sfportscan: proto  { all } \
#                    memcap { 10000000 } \
#                    sense_level { low }   # Roger
preprocessor sfportscan: proto  { ip tcp icmp } \
                    memcap { 10000000 } \
                    sense_level { low } \
                    watch_ip { 196.200.10/25 }\
                    ignore_scanners { 196.201.12.7 196.201.15.6 }\
                    ignore_scanned { 196.201.12.6 196.201.15.7 }
```

Pour cette section (précédente), j'avais deux machines qui foutaient la pagaille dans mon snort avec du SIP à savoir 196.201.12.7 et 196.201.15.6, donc j'ai essayé de diminuer leur

pollution de cette façon. Mais je ne sais plus si c'est ce qui les a calmé, je pense avoir fait autre chose en plus.

Très important ce qui arrive, c'est ce qui va déterminer la manière dont snort store les informations qu'il recueille : soit dans une base de données, ou bien dans des fichiers.
Vous avez ces 3 lignes dans votre fichier :
a - # output alert_syslog: LOG_AUTH LOG_ALERT
b- # output log_tcpdump: tcpdump.log
c- # output database: log, mysql, user=root password=test dbname=db host=localhost

Pour stocker dans /var/log/snort, décommentez l'une des 2 premières lignes
Pour stocker dans une base de données, décommentez la dernière et c'est ce qui est plus intéressant, car c'est avec cette option qu'il faut installer l'ACID. Voici les lignes de mon fichier :
output database: log, mysql, user=root password=test dbname=db host=localhost # Roger
output database: alert, mysql, dbname=snort user=snort host=localhost password=password_for_snort_user_in_mysql

Dans la section **# Step #4: Configure snort with config statements**, rajoutez les ports que vous voulez ignorer comme dans :
Roger a rajouter cette ligne a cause des alertes inutiles pour SIP
config ignore_ports: udp 5060

Le reste du fichier consiste en des include des fichiers de règles, si une règle vous embette beaucoup, mettez en commentaire la ligne dans laquelle on l'appelle.
Exemple :
include $RULE_PATH/icmp.rules # Désactiver le scannage de ICMP
Il y'a aussi le threshold qui est très interessant et qui permet de réduire le nombre lorsqu'elles se répètent trop souvent.

Voilà ! Fin de configuration de snort ; pour ceux qui ont choisi l'installation sans base de données, vous pouvez le lancer avec :
$]# */usr/sbin/snort -A full -d -D -i eth0 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort*

II – Installation de l'interface graphique :

Pour ceux qui ont fait l'installation de snort à base de RPM, il faut installer snort-mysql-2.4.3-xyz.patati.rpm avant d'aller plus loin.

2.1 - Création et configuration de la base mysql snort :

Se connecter au serveur mysql avec les privilèges du root.
$]# mysql –u root -p
> create database snort ;
> grant create, insert, select, delete, update on snort.* to snort ;

> grant create, insert, select, delete, update on snort.* to snort@localhost ;
> set password for snort@localhost=PASSWORD('password_for_snort_user_in_mysql') ;
> set password for snort@%=PASSWORD('password_for_snort_user_in_mysql') ;
> flush privileges ;
> exit
La base de données snort est créée mais sans aucune structure (tables).

Pour créer les tables de la base de données avec un schéma déjà existant :
$]# mysql –u root –p < /chemin/snort-2.4.3/schema/create_mysql snort
Les tables sont ainsi créées.
Pour voir les tables :
$]# mysql –u snort –p
> use snort ;
> show tables ;

2.2 - Installation de l'ACID :

(Je suppose que Apache et php avec php-gd sont installés. Pour des détails sur php-gd, rendez-vous sur http://pear.php.net/)
Téléchargez ADODB sur http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb462.tgz
Puis BASE sur http://easynews.dl.sourceforge.net/sourceforge/secureideas/base-1.2.tar.gz
$]# mv adodb462.tgz /var/www
$]# mv base-1.2.tar.gz /var/www/html
$]# cd /var/www
$]# tar –zxvf adodb462.tgz
$]# rm –f adodb462.tgz
$]# cd html
$]# tar –zxvf base-1.2.tar.gz
$]# rm –f base-1.2.tar.gz
$]# mv base-1.2 snort
$]# cp snort/base_conf.php.dist snort/base_conf.php
$]# vi snort/base_conf.php
Et modifiez les lignes suivantes :

```
//$BASE_Language = "english"; //# Roger
$BASE_Language = "french";

/* $BASE_urlpath = ""; # Roger */
$BASE_urlpath = "/snort";

/* $DBlib_path = ""; # Roger */
$DBlib_path = "/var/www/adodb";

/*$alert_dbname   = "snort_log"; # Roger */
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "password_for_snort_user_in_mysql";
```

Lancement de snort :

$]# */usr/sbin/snort -deyq -c /etc/snort/snort.conf –D –u snort –g snort*
Mettez cette ligne dans **rc.local** si vous le voulez.

Puis dans un navigateur web, tapez : http://<ip_de_la_machine_de_snort>/snort/

Vous aurez une bannière initiale de démarrage ; lire attentivement et cliquer sur « setup page ». Et donc là, c'est la fin, votre snort commence et aboyer et même à mordre.

Un peu de pub pour Mozilla Firefox :