

GUIDE INSTALL IPS

Snort_inline

Snort_inline est une version modifiée de Snort qui fonctionne en tant qu'IPS (Intrusion Prevention System) afin de détecter et bloquer des attaques en temps réel. Les étapes d'installation et de configuration sont testées sous Debian Lenny.





الوكالة الوطنية للأمن المعلوماتية
Agence Nationale de la Sécurité Informatique

Gestion de document

Version	Date	Modification apportée
1.0	08/06/2008	Première version
2.0	08/02/2010	Deuxième version

PLAN

1.	Présentation	3
2.	Installation des prés-requis	3
3.	Installation de snort_inline	5
4.	Configuration.....	6
5.	Tester snort_inline	7
▪	Exemple de test de fonctionnement	8
▪	Lancer Snort_inline en mode démon	9

1. PRESENTATION

Snort_inline communique avec iptables via la bibliothèque libipq. Il emploie des règles (drop, reject...) pour indiquer à iptables si on devrait rejeter, modifier ou laisser passer un paquet.

Le principe de fonctionnement de Snort_inline est le suivant :

- Snort_inline charge une base de signatures d'attaques.
- Lorsqu'un paquet de données entre dans le réseau, Snort_inline le confronte à sa base de signatures afin de vérifier la présence de paquets de réseau malveillants.
- Le noyau s'en charge en poussant les paquets de données dans une file d'attente à l'aide du module ip_queue.
- Snort_inline devrait commencer à traiter les paquets contenus dans l'ip_queue et donc reprendre une activité réseau normale.

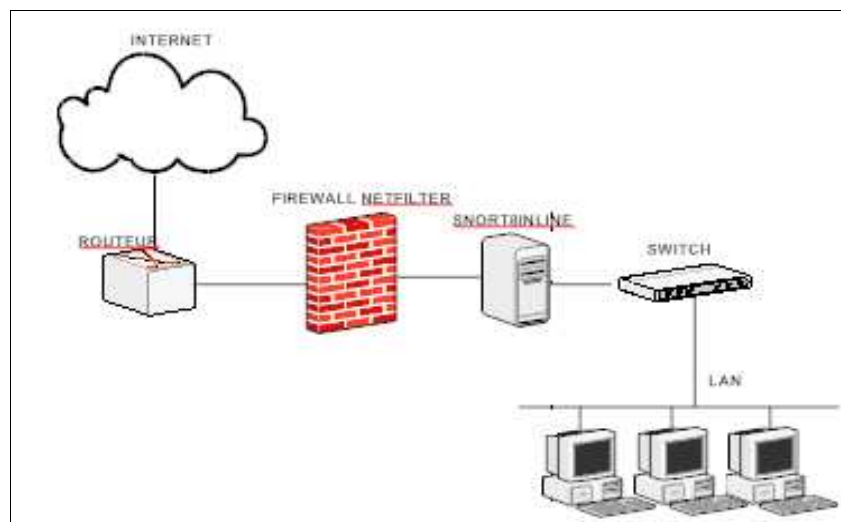


Fig1. Mise en place du snort_inline dans un LAN

2. INSTALLATION DES PRES-REQUIS

Snort_inline exige l'installation des prés requis afin de le configurer sur un système debian. Pour commencer, il faut installer et compiler le code source d'iptables avec l'option « install-devel » afin d'installer la bibliothèque libipq qui permet la communication avec snort_inline.

- 1- Télécharger iptables : <http://www.iptables.org/projects/iptables/downloads.html>

```
cd /usr/src

tar -xzvf iptables-1.4.6.tar.gz

cd iptables-1.4.6

./configure

make

make install
```

- 2- Ensuite, il est nécessaire d'installer et de compiler libnet ; une API (*Application Programming Interface, interface de programmation d'applications*) haut niveau permettant à snort de construire et d'injecter des paquets dans le réseau.

Libnet à télécharger à partir de ce lien : <http://code.google.com/p/ips-builder/downloads/detail?name=libnet-1.0.2a.tar.gz&can=2&q=>

```
cd /usr/src

tar xzvf libnet-1.0.2a.tar.gz

cd /usr/src/Libnet-1.0.2a

./configure

make

make install
```

- 3- Le troisième pré requis que vous deviez installer est le paquetage pcre (*Perl-Compatible Regular Expressions, la bibliothèque d'expressions régulières compatible avec Perl*). <http://sourceforge.net/projects/pcre/files/pcre/8.01/pcre-8.01.tar.gz/download>

```
cd /usr/src
```

```
tar xzvf pcre-8.01.tar.gz

cd /usr/src/pcre-8.01

./configure

Make

make install
```

- 4- Le quatrième pré-requis est Libnet. A télécharger depuis ce lien : <http://libdnet.sourceforge.net>

```
cd /usr/src

tar xzvf libdnet-1.11.tar.gz

cd /usr/src/libdnet-1.11

./configure

make

make install
```

3. INSTALLATION DE SNORT_INLINE

Une fois l'installation des prés requis est terminée sans aucune erreur, vous pouvez maintenant télécharger et installer snort_inline à partir du site : <http://snort-inline.sourceforge.net/>

```
cd /usr/src

tar xzvf snort_inline-2.6.1.5.tar.gz

cd snort_inline-2.6.1.5

./configure
```

```
make  
  
make install
```

- Faites un enregistrement dans le site de snort.org pour avoir une clé oinkmaster afin de l'utiliser pour les téléchargements des rules.
- Dans le répertoire « `/etc/snort` » faites :

```
wget http://www.snort.org/pub-bin/oinkmaster.cgi/<clé oinkmaster>/snortrules-  
snapshot-2.8.tar.gz  
  
tar xvf snortrules-snapshot-2.8.tar.gz  
  
cp ../rules /usr/src/snort_inline-2.6.1.5/
```

4. CONFIGURATION

- Tout d'abord, il faut modifier le fichier de configuration de `snort_inline`, en le faisant pointer sur le chemin correct pour pouvoir obtenir ses règles.

```
cd /usr/src/snort_inline-2.6.1.5  
  
cp /usr/src/snort_inline-2.6.1.5/etc/classification.config /usr/src/snort_inline-2.6.1.5  
/rules/  
  
cp /usr/src/snort_inline-2.6.1.5/etc/reference.config /usr/src/snort_inline-2.6.1.5 /rules/
```

- Ensuite Déplacez les fichiers de configuration et de définition de règles dans le répertoire `/etc.`, où résident habituellement les fichiers de ce type :

```
mkdir /etc/snort_inline  
  
cp /usr/src/snort_inline-2.6.1.5 /etc/* /etc/snort_inline/  
  
cp /usr/src/snort_inline-2.6.1.5 /rules /etc/snort_inline/ -R
```

- Puis, vous devez vérifier maintenant les chemins d'accès aux règles dans le fichier « `/etc/snort_inline/snort_inline.conf` ». Editez ce fichier et modifiez la ligne suivante :

```
var RULE_PATH /etc/snort_inline/drop_rules
```

```
par
```

```
var RULE_PATH /etc/snort_inline/rules
```

- Créez un répertoire pour les logs de snort_inline:

```
mkdir /var/log/snort_inline
```

- Le noyau s'en charge en poussant les données dans une file d'attente à l'aide du module ip_queue. Vous pouvez charger ip_queue et vérifier sa présence comme suit :

```
modprobe ip_queue
```

```
lsmod | grep ip_queue
```

Si la ligne suivante est affichée alors le module est actif :

```
ip_queue 10368 0
```

- Enfin, iptables doit être configuré pour envoyer le trafic à ip_queue. Cette redirection s'effectue à l'aide de la ligne suivante, qui redirige tous les paquets de réseau destinés au port 80 vers le module ip_queue.

```
iptables -I INPUT -p tcp --dport 80 -j QUEUE
```

Il est alors facile de vérifier le fonctionnement d'iptables. Votre navigateur se bloque, c'est parce que tous les paquets sont routés vers ip_queue et attendent d'être libérés par iptables.

5. TESTER SNORT_INLINE

Snort_inline peut maintenant être lancé à l'aide de la commande ci-dessous et avec les options suivantes:

- « c » chemin de fichier de configuration : afin de spécifier quels sont les règles qui seront actifs.
- « Q » : permet d'employer le module ip_queue pour iptables.
- « N » : signifie que les alertes ne seront pas loggées.

- « l » : enregistre les logs dans le répertoire /var/log/snort_inline
- « v » : affiche le fonctionnement de snort_inline en mode verbose

```
snort_inline -c /etc/snort_inline/snort_inline.conf -Q -N -l /var/log/snort_inline -v
```

Vous devriez voir du texte défiler et snort_inline affiche un message semblable à celui-ci :

```
__== Initialisation Complete ==__
```

Snort_inline fonctionne à présent. Il devrait commencer à traiter les paquets contenus dans la liste d'attente ip_queue et donc reprendre une activité réseau normale.

▪ Exemple de test de fonctionnement

Dans cet exemple, nous allons rejeter toute l'activité sur le port 80.

- 1- Essayez de vous connecter via votre navigateur web. Vous devriez à présent voir la page web que vous attendiez.
- 2- Maintenant ajoutez une règle de test de façon que vous puissiez voir si snort_inline fonctionne réellement. Pour ce faire, éditez le fichier /etc/snort_inline/rules/web-attacks.rules et ajoutez la règle suivante avant la première instruction « alert », mais au-dessous des commentaires.

```
Drop tcp any any -> any 80 (classtype:attempted-user ; msg:"port 80
connection initiated";)
```

- 3- Relancez Snort_inline à nouveau.

```
Ps -ef | grep snort_inline
```

```
Kill -9 "pid"      # le pid de snort_inline qui a été affiché par la commande
précédente
```

```
snort_inline -c /etc/snort_inline/snort_inline.conf -Q -N -l /var/log/snort_inline -v
```

- 4- Essayez encore une fois de reconnecter à cette page web. Votre requête devrait maintenant échouer.

- 5- Vérifiez les fichiers journaux, pour voir si snort_inline a capturé le « paquet malveillant ». Sur la machine où s'exécute snort_inline, appuyez sur Ctrl+c une fois de plus pour arrêter le processus snort_inline ou par la commande kill cité ci-dessus et saisissez la commande suivante :

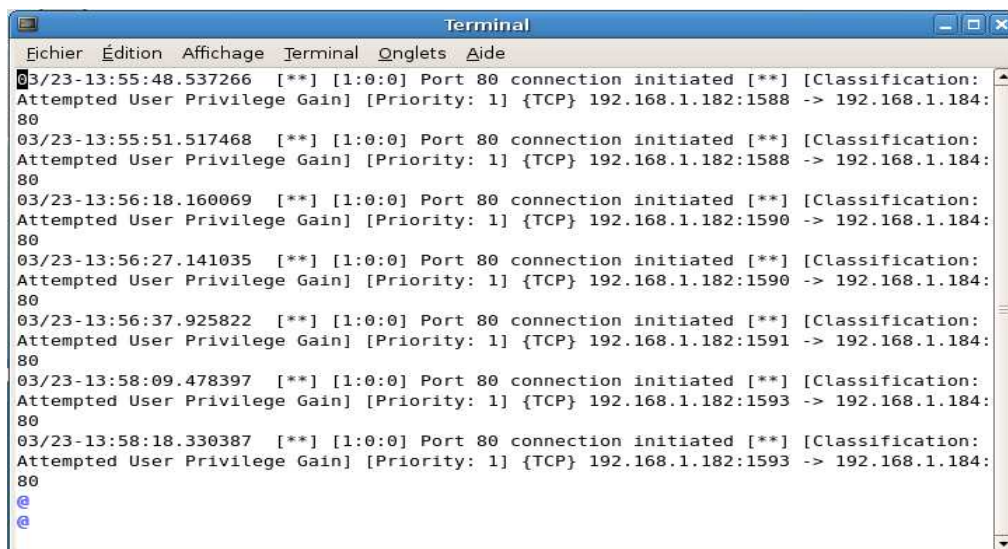
```
cat /var/log/snort_inline/snort_inline_full
```

Ou vous pouvez également afficher une version plus courte, en émettant la commande suivante :

```
cat /var/log/snort_inline/snort_inline_fast
```

- Cette commande devrait afficher un message semblable à celui-ci :

«**Port 80 connection initiated**», c'était la ligne que vous avez saisie dans le champ « msg » de la règle ajoutée ci-dessus.



■ Lancer Snort_inline en mode démon

Pour pouvoir utiliser snort_inline efficacement:

- Vous devez maintenant supprimer la règle de rejet ajoutée ci dessus.
- Puis modifier tous les fichiers de règles, en transformant les règles d'alerte en règle de rejet. Une commande simple peut suffire, mais il faut la

saisir avec exactitude. (Faites une sauvegarde de votre dossier de règles avant de saisir cette commande).

```
cd /etc/snort_inline/rules/

for file in $(ls -1 *.rules)

do

    sed -e 's:^alert:drop:g' ${file} > ${file}.new

    mv ${file}.new ${file} -f

done
```

- Il ne reste plus qu'à exécuter snort_inline en tant que démon avec la ligne suivante, la seule différence étant la présence du *-D* qui signifie que snort_inline fonctionne en mode daemon:

```
snort_inline -c /etc/snort_inline/snort_inline.conf -Q -N -l /var/log/snort_inline -v -D
```