Installation de Snort en manuel

Installation des paquets nécessaire au fonctionnement de snort

Une fois que le système est à jour il faut installer les paquets suivants dont snort a besoin pour fonctionner. Via la commande apt-get install.

- flex
- bison
- build-essential
- checkinstall
- libpcap-dev
- libnet1-dev
- libpcre3-dev
- libnetfilter-queue-dev
- iptables-dev
- libdumbnet-dev
- zlib1g-dev
- tcpdump

Il est possible d'installer tous les paquets via une seule commande.

```
apt-get install tcpdump flex bison build-essential checkinstall libpcap-dev libnet1-dev libpcre3-dev libnetfilter-queue-dev iptables-dev libdumbnet-dev zlib1g-dev -y
```

Installation de la bibliothèque d'acquisition des données

Pour installer snort, il va falloir récupérer les fichiers d'installation présents sur le site officiel, les décompresser, enfin les installer.

1 Création du dossier de stockage

Dans un premier temps créez un dossier où seront stockés les fichiers d'installation snort après le téléchargement. La création du dossier se fait par la commande

```
mkdir /usr/src/snort_src
```

Ensuite placez-vous dans le dossier créé avec la commande

```
cd /usr/src/snort_src
```

2 Téléchargement la bibliothèque d'acquisition des données

Pour télécharger le fichier de la bibliothèque d'acquisitions des données il suffit d'utiliser la commande

```
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
```

3 Décompression du fichier

Une fois le fichier téléchargé il faut décompresser l'archive

```
 tar xvfz daq-2.0.7.tar.gz
```

4 Installation et configuration de la bibliothèque d'acquisition des données

Apres la décompression, il faut se rendre dans le répertoire crée suite à la décompression. Ensuite il faut lancer l'installation et la configuration

```
cd daq-2.0.7/
./configure
make
sudo make install.
```

Installation de snort

1. Téléchargement de snort

   ```
   wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz
   ```

2. Décompression du fichier snort

   ```
   tar xvfz snort-2.9.20.tar.gz
   ```

3. Installation et configuration de snort

   ```
    cd snort-2.9.20
   ```

4. Ensuite il faut lancer l'installation et la configuration

   ```
    ./configure --enable-sourcefire; make; make install
   ```

5 Vérification de l'installation snort

Pour vérifier que la bibliothèque partagée soit bien à jour on peut utiliser la commande

```
sudo ldconfig
```

Enfin il est possible de test l'installation snort avec la commande

```
snort —-version
```

le résultat attendu est le suivant.

6 Création d'un utilisateur snort

Afin d'éviter que snort se lance en utilisateur root ce qui donne accès à de nombreux privilèges. Il faut donc créer un utilisateur snort.

```
groupadd snort
useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

7 Création des dossiers de configuration

Les commandes suivantes vont créer des fichiers dans des répertoires différents.

- dossier qui contient les fichiers de configuration snort :

```
mkdir /etc/snort
```

Les commandes suivantes vont créer des dossiers pour différents types de règles.

```
mkdir /etc/snort/rules
mkdir /etc/snort/preproc_rules
touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
/etc/snort/rules/local.rules
mkdir /usr/local/lib/snort_dynamicrules
```

Enfin il faut créer le dossier qui va contenir les logs.

```
mkdir /var/log/snort
```

Attribution des droits

Suite à la création des différents fichiers il faut leur donner des droits sur les dossiers. Utilisateur : lecture/écriture/exécution Groupe : lecture/écriture/exécution Autre : lecture/exécution

```
chmod -R 5775 /etc/snort
chmod -R 5775 /var/log/snort
chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

On ajoute l'utilisateur snort et groupe aux différents dossiers.

```
chown -R snort:snort /etc/snort
chown -R snort:snort /var/log/snort
```

```
chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

8 Copie des fichiers de configuration

Lors de l'installation les fichiers ont été crééqsdans le répertoire */usr/src/snort_src/* on va donc copier vers le dossier /etc/snort.

```
cp /usr/src/snort_src/snort*/etc/*.conf* /etc/snort
sudo cp /usr/src/snort_src/snort*/etc/*.map /etc/snort
```

Configuration snort

1 Configuration du réseau à sécuriser

Dans le fichier snort.conf il va falloir configurer la variable *ipvar HOME_NET* avec l'adresse IP réseau.

Le fichier se trouve dans le répertoire ***/etc/snort/*** pour ouvrir le fichier *snort.conf*.

De plus il faut laisser la variable *ipvar EXTERNAL_NET* avec l'option *any*. Cette variable concerne le réseau externe.

Il est possible de lister les adresses IP des serveurs dns présents sur le réseau avec la variable *ipvar DNS_SERVERS*.

2 Configuration des chemins snort

Les fichiers sont dans un répertoire il faut donc indiquer le chemin pour aller récupérer.

Les chemins a configurer sont les suivants dans les encadrés jaune.

Les cinq chemins qu'il faut modifier avec les répertoires suivants.

```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

De plus Il va falloir commenter les règles **à partir de la ligne 548 jusqu'à la ligne 652** du fichier *snort.conf*.