Snort

Snort est un système de détection d'intrusion libre publié sous licence GNU GPL

1. Installation

```
#apt install snort
```

On configure ensuite le réseau à surveiller:
/etc/snort/snort.debian.conf

```
DEBIAN_SNORT_HOME_NET="<@Réseau/CIDR>"
DEBIAN_SNORT_INTERFACE="<IntName>"
```

Cette donnée se retrouve par la suite dans les règles sous la variable $HOME_NET .

2. Règles

Snort possède des règles configuré par défaut dans */etc/snort/rules/* . Un fichier est présent ce dossier nous permettant de renseigner nos propres règles (*local.rules*).

Syntaxe d'une règle:

```
Action Protocol Networks Ports Direction Operator Networks Ports (RULE_OPTIONS)
```

Exemple:

```
alert icmp any any -> $HOME_NET any (msg:"Tentative connexion ICMP"; sid:00001;
rev:1;)
```

Pour plus d'information sur la création de règles, se référer aux documentations:
https://www.snort.org/documents#OfficialDocumentation.

3. Test

A titre d'exemple, on va créer une alerte pour tout paquet ICMP sur le réseau.

On ajoute cette ligne dans le fichier */etc/snort/rules/local.rules* :

```
alert icmp any any -> $HOME_NET any (msg:"Tentative connexion ICMP"; sid:00001;
rev:1;)
```

On lance snort en redirigeant les alertes vers le terminal:

```
# snort -A console -i eth0 -u snort -c /etc/snort/snort.conf
```

Ensuite, on ping une ip du réseau:

```
# ping <IPprivée>
```

Résultat:

```
02/10-14:11:01.621602  [**] [1:1:1] Tentative connexion ICMP [**] [Priority: 0] {ICMP} 172.17.0.59 -> 172.17.0.218
02/10-14:11:01.621605  [**] [1:1:1] Tentative connexion ICMP [**] [Priority: 0] {ICMP} 172.17.0.59 -> 172.17.0.218
```

L'ensemble des alertes/logs de snort sont stockés dans */var/log/snort*. Pour accéder à un fichier de log, exécutez la commande suivante :

```
# snort -r /var/log/snort/snort.log.xxxxxx
```