TP Snort



Sommaire

١.	Ir	ntroduction
II.	С	onfiguration requise3
III.		Installation et configuration4
1))	Préparation de l'environnement et installation des dépendances5
2))	Installation de DAQ (Data Acquisition Library)5
3))	Téléchargement et installation de Snort 3.5.05
4))	le mode promiscuous6
5))	l'interface Offloading6
6))	Rendre les changements permanents7
	1	. Activer le mode promiscuous au démarrage7
7))	Configuration de base de Snort8
8))	Teste de la configuration9
IV.		Test10
1))	Démarrer Snort10
2))	Lancer un ping depuis une autre machine10
3))	Vérifier les messages10
V.	С	onclusion

I. Introduction

C'est un système de détection d'intrusion (IDS) : dispositif (sous forme de sondes branchées sur le réseau) ou logiciel conçu pour surveiller le trafic réseau ou les activités système à la recherche de comportements suspects en temps réel.

Snort intégre aussi une solution de prévention d'intrusion (IPS).

II. Configuration requise

Prérequis généraux pour Snort (dernière version 3.x)

1. 🤤 Système d'exploitation compatible

Snort tourne sous :

- Linux (Debian, Ubuntu, CentOS, RHEL... recommandé)
- FreeBSD
- Peut être compilé sous Windows, mais c'est plus complexe (déconseillé en prod)

👉 La plupart des gens installent Snort sur **Ubuntu Server** ou **CentOS/RHEL**.

2. 🌾 Dépendances logicielles

Avant d'installer Snort, tu dois avoir certains paquets installés : « apt install -y git wget build-essential libpcap-dev libpcre3-dev \ libdumbnet-dev zlib1g-dev libluajit-5.1-dev libssl-dev cmake libunwind-dev \ luajit hwloc bison flex liblzma-dev openssl pkg-config libhwloc-dev \ cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev \ libmnl-dev autotools-dev libfl-dev libgoogle-perftools-dev ethtool» (Selon la version de Linux, les noms peuvent légèrement changer) Snort 3 utilise aussi DAQ (Data Acquisition library), donc tu dois aussi l'installer.

3. 💾 Configuration matérielle minimale

Pour un environnement de test/labo :

Ressource Minimum

CPU 2 cœurs

RAM 4 Go

Ressource Minimum

Stockage 20 Go

Réseau 1 Gbit

Pour un usage en production, ça dépend beaucoup du trafic réseau que tu veux analyser :

Nombre d'hôtes	S CPU	RAM	Stockage (logs)
< 100	4 cœurs	8 Go	100+ Go
100 - 1000	8+ cœurs	16 Go	500 Go – 1 To
> 1000	16+ cœurs	32+ Go	SSD + 1 To+

4. 🧠 Autres prérequis utiles

- Interface réseau dédiée en mode promiscuité pour le sniffing.
- Optionnel : installation de **Barnyard2** (pour gestion de logs) ou **Base/Snorby** pour l'interface web.
- Un outil de gestion des règles : **PulledPork** ou **Snort Subscriber Rules** (si tu veux les règles officielles à jour).

III. Installation et configuration

- Ubuntu à jour
- Installation des dépendances : build-essential bison libpcre3-dev zlib1g-dev libpcap-dev libdumbnet-dev flex
- Télecharger et installer la dernière version sur snort.org
- Fichier de configuration dans /Etc/snort
 - o Snort.conf :fichier principal
 - Local.rules : règles spécifiques à votre réseau
 - Classification.config : catégories d'alertes et gravité
 - Threshold.conf : seuils pour limiter les alertes répétitives
- Dans snort.conf : réseau interne et externe

Var HOME_NET 192.168.X.0/24 Var EXTERNAL_NET any Include \$RULE_PATH/local.rules

- Dans local.rules :exemple de règle
 Alert tcp any any ->\$HOME_NET 80 (msg : « Tentative de connexion http. » ;sid :1
 000 001 ;rev :1)
- Lancement du server : snort -c /etc/snort/snort.conf -i eth0 -A console ou snort -c /etc/snort/snort.conf -i eth0 -I /var/log/snort -D

1) Préparation de l'environnement et installation des dépendances

On commence par installer les dépendances nécessaires (seules celles-ci sont vraiment importantes ce qu'il y a écrire tout en haut moins) avec la commande « sudo apt install build-essential bison libpcre3-dev zlib1g-dev libpcap-dev libdumbnet-dev flex »

loic@loic-VirtualBox:~\$ sudo apt install build-essential bison libpcre3-dev zlib
1g-dev libpcap-dev libdumbnet-dev flex

2) Installation de DAQ (Data Acquisition Library)

Maintenant, on va installer le DAG (Data Acquisition Library). Pour ce faire on va faire la commande « git clone https://github.com/snort3/libdaq.git »

loic@loic-VirtualBox:~\$ git clone https://github.com/snort3/libdaq.git
Clonage dans 'libdaq'...

Puis la commande « cd libdaq

./bootstrap

./configure

make

sudo make install

Idconfig » avec les droits administrateurs.

```
loic@loic-VirtualBox:~$ sudo su
root@loic-VirtualBox:/home/loic# cd libdaq
./bootstrap
./configure
make
sudo make install
ldconfig
```

3) Téléchargement et installation de Snort 3.5.0

Maintenant, on télécharge Snort 3.5.0 depuis le site officiel avec « cd ..

wget https://github.com/snort3/snort3/archive/refs/tags/3.5.0.0.tar.gz »

```
root@loic-VirtualBox:/home/loic/libdaq# cd ..
wget https://github.com/snort3/snort3/archive/refs/tags/3.5.0.0.tar.gz
--2025-04-21 17:06:36-- https://github.com/snort3/snort3/archive/refs/tags/3.5.
0.0.tar.gz
```

On extraie l'archive avec « tar -xzvf 3.5.0.0.tar.gz

```
cd snort3-3.5.0.0 ».
```

root@loic-VirtualBox:/home/loic/snort3-3.5.0.0# tar -xzvf 3.5.0.0.tar.gz
cd snort3-3.5.0.0

On configure Snort en incluant les options pour gperftools et DAQ « ./configure_cmake.sh -- prefix=/usr/local --enable-tcmalloc »

root@loic-VirtualBox:/snort3-3.5.0.0# ./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc

Compliez et installez Snort avec « cd build

make

make install

Idconfig »



Vérifiez l'installation de Snort : avec « snort - V ».



4) le mode promiscuous

Maintenant, on va activer le mode promiscuous. C'est un mode spécial des interfaces réseau qui permet à une machine de voir tout le trafic qui passe sur le réseau, pas seulement celui qui lui est destiné. À savoir que pour les commandes suivantes, il faut connaître le nom de l'interface de votre machine, pour ça vous pouvez faire la commande « ip a » sur Ubuntu.

Pour activer le mode promiscuous sur l'interface réseau enp0s3, exécutez la commande suivante : « sudo ip link set enp0s3 promisc on ».

```
root@loic-VirtualBox:/snort3-3.5.0.0/build# sudo ip link set enp0s3 promisc on
```

Vérifiez que l'interface est bien en mode promiscuous avec la commande suivante : « ip link show enp0s3 »

гоо	@loic-VirtualBox:/home/loic# ip link show enp0s3
2:	np0s3: <broadcast,multicast,promisc,up,lower_up> mtu 1500 qdisc fq_codel st</broadcast,multicast,promisc,up,lower_up>
te	IP mode DEFAULT group default qlen 1000
	link/ether 08:00:27:28:52:32 brd ff:ff:ff:ff:ff:ff

On peut voir la mention « PROMISC » qui montre que l'interface et bien en mode promiscuous.

5) l'interface Offloading

Après avoir activé le mode promiscuous on va désactiver l'interface Offloading.

L'interface offloading permet à la carte réseau de gérer certaines tâches automatiquement pour améliorer les performances.

Mais pour Snort, ça fausse l'analyse du trafic, car les paquets sont modifiés avant d'être inspectés. Donc, on désactive le offloading pour s'assurer que Snort voie les paquets bruts, exactement comme ils circulent sur le réseau.)

On doit donc désactiver les fonctionnalités GRO et LRO.

Avant de les désactiver il faut vérifier si GRO et LRO sont activés, exécutez la commande suivante : « ethtool -k enp0s3 | grep -E 'generic-receive-offload|large-receive-offload' »

```
root@loic-VirtualBox:/home/loic# ethtool -k enp0s3 | grep -E 'generic-receive-of
fload|large-receive-offload'
generic-receive-offload: on
large-receive-offload: off [fixed]
```

Si vous voyez « on [fixed] » pour l'une de ces options, cela signifie que l'interface réseau ne permet pas de les désactiver, et il pourrait être nécessaire de changer de matériel ou d'interface si ce problème persiste.

Pour désactiver GRO et LRO il faut faire les commandes : « ethtool -K enp1s0 gro off et ethtool -K enp1s0 lro off »

```
root@loic-VirtualBox:/home/loic# ethtool -K enp0s3 gro of
ethtool -K enp0s3 lro off
```

Vérifiez de nouveau les paramètres pour vous assurer que GRO et LRO sont bien désactivés : « ethtool -k enp1s0 | grep -E 'generic-receive-offload|large-receive-offload'

```
generic-receive-offload: off
```

```
large-receive-offload: off [fixed] »
```

```
root@loic-VirtualBox:/home/loic# ethtool -k enp0s3 | grep -E 'generic-receive-of
fload|large-receive-offload'
generic-receive-offload: off
large-receive-offload: off [fixed]
```

- 6) Rendre les changements permanents
- 1. Activer le mode promiscuous au démarrage

Créez ou éditez un fichier de service pour appliquer cette configuration au démarrage. Par exemple, créez un script dans /etc/systemd/system/promisc-mode.service : « sudo nano /etc/systemd/system/promisc-mode.service »

root@loic-VirtualBox:/home/loic# sudo nano /etc/systemd/system/promisc-mode.service

Ajoutez-y les lignes suivantes :

GNU nano 7.2	<pre>/etc/systemd/system/promisc-mode.service *</pre>					
[Unit]						
Description=Set Snort 3 NIC in promiscuo	us mode and Disable GRO, LRO on boot					
After=network.target						
[Service]						
Type=oneshot						
ExecStart=/usr/sbin/ip link set dev enp1s0 promisc on						
ExecStart=/usr/sbin/ethtool -K enp1s0 gro off lro off						
TimeoutStartSec=0						
RemainAfterExit=yes						
[Install]						
WantedBy=default.target						
EOL						

Activez ensuite le service pour qu'il démarre automatiquement : « sudo systemctl enable promiscmode.service ».

root@loic-VirtualBox:/home/loic# sudo systemctl enable promisc-mode.service

7) Configuration de base de Snort

Pour commencer la configuration de Snort on va ouvrir et éditer le fichier de configuration. Le fichier de configuration par défaut pour Snort 3 est un fichier Lua généralement situé dans /usr/local/etc/snort/snort.lua

Commencez par ouvrir ce fichier dans un éditeur de texte : « sudo nano /usr/local/etc/snort/snort.lua ».

root@loic-VirtualBox:/home/loic# sudo nano /usr/local/etc/snort/snort.lua

Dans le fichier de configuration on va spécifiez l'interface réseau à surveiller, il faut donc chercher la partie qui définit l'interface réseau et modifiez-la pour qu'elle pointe vers votre interface réseau :

« "-- Interface à surveiller

interface = "enp1s0" ».

Toujours dans le même fichier on va définir les variables HOME_NET et EXTERNAL_NET.



Encore une fois dans le fichier il faut activer les règles de détection.



Maintenant on va créer une règle. Pour commencer, il faut créer les dossiers et les fichiers nécessaires : « mkdir /usr/local/etc/rules

mkdir /usr/local/etc/so_rules/

mkdir /usr/local/etc/lists/

touch /usr/local/etc/rules/local.rules

touch /usr/local/etc/lists/default.blocklist

mkdir /var/log/snort ».



Editez le fichier local.rules pour y ajouter la règle suivante : « alert icmp any any -> \$HOME_NET any (msg:"Ping ICMP détecté"; sid:1000001; rev:1;) »

```
alert icmp any any -> $HOME_NET any (msg:"Ping ICMP détecté"; sid:1000001; rev:1;)
```

8) Teste de la configuration

Avant de lancer Snort en mode de détection, vérifiez que le fichier de configuration ne contient pas d'erreurs : sudo snort -T -c /usr/local/etc/snort/snort.lua -i enp0s3.



IV. Test

1) Démarrer Snort

Pour que la nouvelle règle soit prise en compte, Démarrez Snort en spécifiant le fichier de configuration, le fichier de règles et l'interface à surveiller : « sudo snort -c

/usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules -i enp1s0 -A alert_fast -s 65535 -k none »

2) Lancer un ping depuis une autre machine

Depuis une autre machine sur le même réseau, envoyez un ping vers l'adresse IP de la machine sur laquelle Snort est configuré. Par exemple : « ping X.X.X.X »

```
C:\Users\corne382673>ping 10.0.2.15
```

3) Vérifier les messages

Sur la machine où a été lancé Snort, vérifiez les messages d'alerte dans la sortie standard.

V. Conclusion

Snort est un système de détection d'intrusion (IDS) puissant, flexible et open source, largement utilisé dans le domaine de la cybersécurité. Il permet de surveiller le trafic réseau en temps réel, de détecter des comportements suspects ou malveillants, et de générer des alertes en fonction de règles personnalisées.

Son installation demande de configurer correctement l'environnement, les dépendances, l'interface réseau (souvent en mode promiscuous), et les fichiers de règles. Bien que sa mise en place puisse être complexe, notamment avec les erreurs de configuration comme dans le fichier snort.lua, une fois opérationnel, Snort constitue une solution robuste pour l'analyse et la sécurisation d'un réseau.