

## Installation de Snort 2 (Ubuntu)





## Sommaire :

- 1- Prérequis
- 2- MAJ des paquets
- 3- Installation de snort via apt-get
- 4- Mise en pratique
- 5- Consulter les alertes Snort

# Configuration serveur Snort

## 1- Prérequis

Snort est un système de détection d'intrusion (IDS) open source qui analyse le trafic réseau en temps réel pour identifier des comportements malveillants ou suspects. Il utilise des règles pour détecter des attaques, des intrusions ou des activités non autorisées sur le réseau. Snort peut aussi être configuré en mode préventif (IPS), où il bloque activement les menaces détectées.

## 2- Mise à jour des paquets du système :

Commençons par un update :

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

      .-/+00ssssso+/-.
      `:+ssssssssssssssssss+:`
      -+ssssssssssssssssssyyssst-
      .ossssssssssssssssssdMMMMNysssoo.
      /ssssssssssshdmmNNmmyNNMMMyhsssss/
      +ssssssssshmydMMMMMMNdssssssssst+
      /ssssssssshNNMMMyhyhyhmmNNMMNhssssss/
      .ssssssssdMMMNhssssssssshNNMMMdssssss.
      +ssssshhhyNNMMNyssssssssssyNNMMYssssssst+
      ossyNNMMNyMMhssssssssssshmmhssssssso
      ossyNNMMNyMMhssssssssssshmmhssssssso
      +ssssshhhyNNMMNyssssssssssyNNMMYssssssst+
      .ssssssssdMMMNhssssssssshNNMMMdssssss.
      /ssssssssshNNMMMyhyhyhmmNNMMNhssssss/
      +ssssssssshmydMMMMMMNdssssssssst+
      /ssssssssshdmmNNmmyNNMMMyhsssss/
      .ossssssssssssssssssdMMMMNysssoo.
      -+ssssssssssssssssssyyssst-
      `:+ssssssssssssssssss+:`
      .-/+00ssssso+/-.

sacha@sacha
-----
OS: Ubuntu 24.04.2 LTS x86_64
Host: VirtualBox 1.2
Kernel: 6.11.0-17-generic
Uptime: 5 mins
Packages: 1535 (dpkg), 10 (snap)
Shell: bash 5.2.21
Resolution: 1280x800
Terminal: /dev/pts/1
CPU: 12th Gen Intel i5-12400F (2) @ 2.496GHz
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 920MiB / 3915MiB

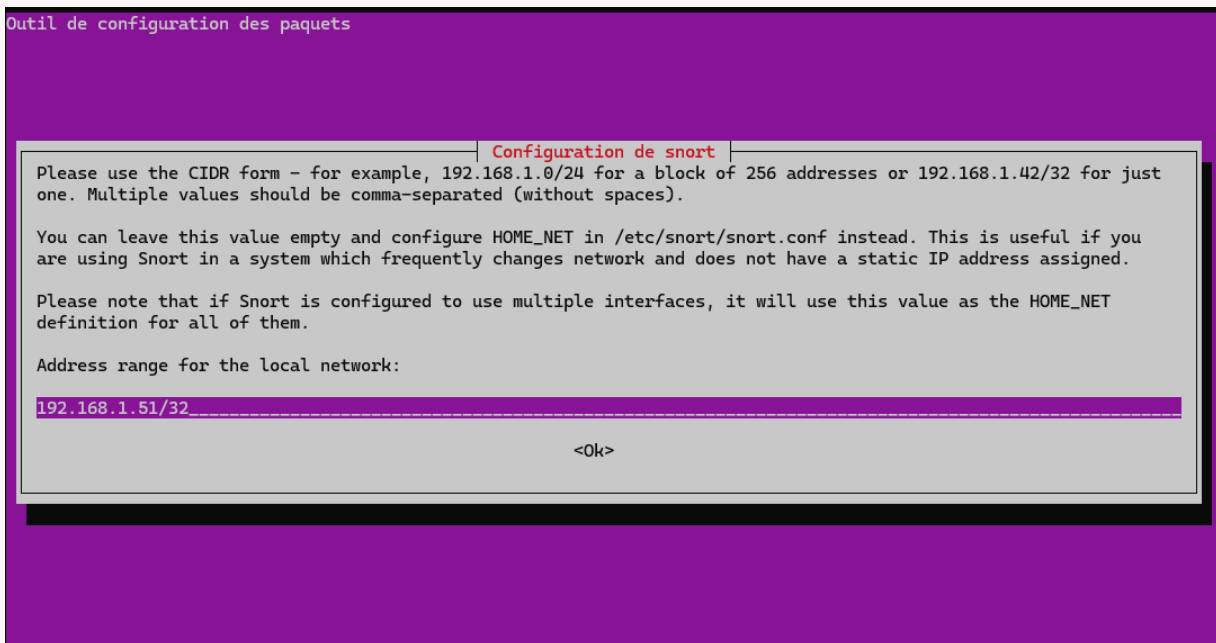
sacha@sacha:~$ sudo apt update
```

# Configuration serveur Snort

## 3- Installation de snort via apt-get :

```
sacha@sacha:~$ sudo apt-get install snort -y
Lecture des listes de paquets... Fait
```

Puis Snort nous demande l'@ip ou le réseau à analyser dans notre cas je vais salement analyser le Traffic de l'@ip de ma machine virtuelle



```
sacha@sacha:~$ snort -V

  '-~
o"  )~
  "'

->* Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
```

# Configuration serveur Snort

## 4- Mise en pratique :

Nous allons maintenant tester une règle que nous allons installer nous même pour cela il faut vérifier la source des fichiers pour les règles local Snort :

```
sacha@sacha:~$ sudo nano /etc/snort/snort.conf
```

```
# site specific rules
include $RULE_PATH/local.rules
```

Nous allons maintenant modifier le fichier :

```
sacha@sacha:~$ sudo nano /etc/snort/rules/local.rules
```

Les règles doivent être écrite de cette façon :

**action protocol sourceIP sourceport -> destinationIP destinationport ([Rule options])**

Pour le test nous allons crée une alerte ICMP

```
GNU nano 7.2 /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP Detection Rule"; sid:100001;)
```

# Configuration serveur Snort

## 5- Consulter les alertes Snort :

Pour consulter les alertes Snort en temps réel il est possible de faire de cette façon :

***sudo Snort -T -i ens33 -c /etc/Snort/Snort.conf***

```
sacha@sacha:~$ sudo snort -q -l /var/log/snort/ -i enp0s3 -A console -c /etc/snort/snort.conf
```

Nous pouvons maintenant constater que des alertes ICMP apparaissent :

<pre>sacha@sacha:~\$ sudo snort -q -l /var/log/snort/ -i enp0s3 -A console rt/snort.conf 02/17-17:35:10.867845  [**] [1:100001:0] "ICMP Detection Rule" [**] ] {ICMP} 192.168.1.4 -&gt; 192.168.1.51 02/17-17:35:10.867872  [**] [1:100001:0] "ICMP Detection Rule" [**] ] {ICMP} 192.168.1.51 -&gt; 192.168.1.4 02/17-17:35:11.870757  [**] [1:100001:0] "ICMP Detection Rule" [**] ] {ICMP} 192.168.1.4 -&gt; 192.168.1.51 02/17-17:35:11.870775  [**] [1:100001:0] "ICMP Detection Rule" [**] ] {ICMP} 192.168.1.51 -&gt; 192.168.1.4 02/17-17:35:12.873736  [**] [1:100001:0] "ICMP Detection Rule" [**] ] {ICMP} 192.168.1.4 -&gt; 192.168.1.51 02/17-17:35:12.873754  [**] [1:100001:0] "ICMP Detection Rule" [**]</pre>	<pre>C:\Users\Sacha&gt;ping 192.168.1.51  Envoi d'une requête 'Ping' 192.168.1.51 avec 32 octets de données : Réponse de 192.168.1.51 : octets=32 temps&lt;1ms TTL=64 Réponse de 192.168.1.51 : octets=32 temps&lt;1ms TTL=64 Réponse de 192.168.1.51 : octets=32 temps&lt;1ms TTL=64  Statistiques Ping pour 192.168.1.51:     Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),     Durée approximative des boucles en millisecondes :         Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms  Ctrl+C ^C C:\Users\Sacha&gt;</pre>
--	---