

Mise à **jour Snort 2.9+** : désormais le tutoriel ci-dessous pourrait être devenu **obsolète**. Snort est passé à la version 3 avec un changement complet sous-jacent (dont la moindre prise en charge des systèmes 32bits). La version 2.9 n'est sans doute plus disponible sur votre système s'il est récent, et l'installation pourrait donc ne pas se terminer correctement. Si jamais vous avez trouvé une piste, n'hésitez pas à nous en faire part, en attendant une mise à jour complète du tutoriel.

### Installation de Snort sous Kali Linux

Il est certes un peu déroutant d'installer un système de détection d'intrusion sur une machine d'attaquant, mais nous allons nous baser sur Kali car les étapes sont les mêmes que sur les machines Ubuntu ou Debian. L'installation sur Metasploitable aurait été plus judicieuse, et vous pouvez la tenter de votre côté. Cela dit, elle a posé plusieurs soucis de mon côté et je l'ai donc abandonnée.

### Pourquoi Snort ?

Snort est l'un des systèmes de détection d'intrusion réseau parmi les plus populaires. Il s'agissait initialement d'un renifleur réseau, qui a été amélioré au fil des années grâce à la communauté OpenSource est qui est à présent l'une des références du domaine. De plus il est gratuit.

### Première étape : installer Snort via le dépôt

L'installation est très simple, elle est détaillée sur le site officiel <https://www.snort.org/>.

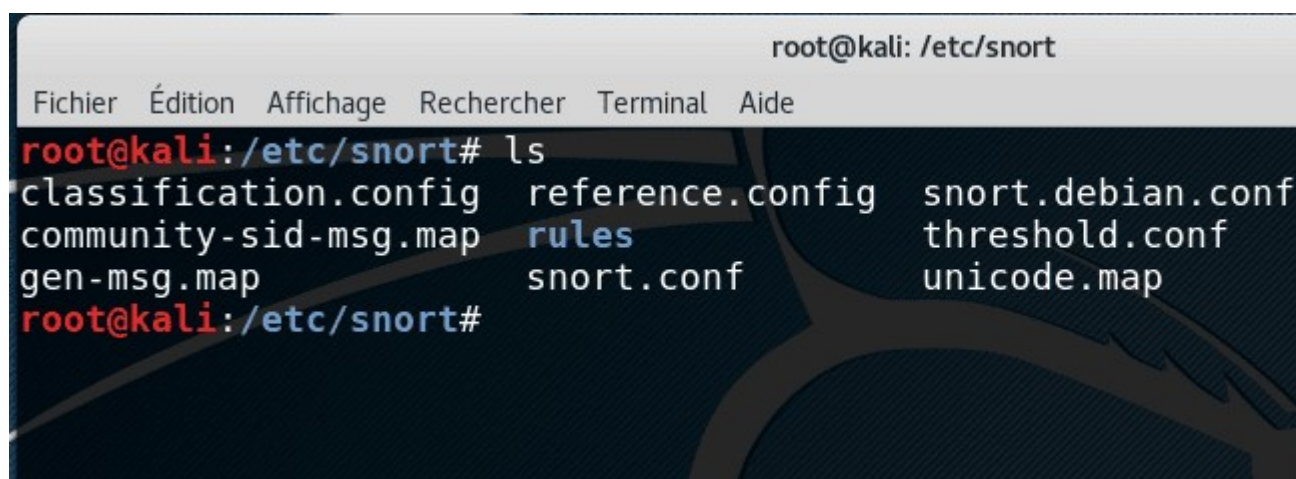
Cela dit, nous allons prendre un raccourci pour l'installer et utiliser directement la commande suivante :

```
sudo apt-get install snort
```

Si cela ne fonctionne pas, nous allons d'abord éditer le fichier `/etc/apt/sources.list` et y ajouter les lignes suivantes :

```
deb http://ch.archive.ubuntu.com/ubuntu/ saucy main restricted
deb-src http://ch.archive.ubuntu.com/ubuntu/ saucy main restricted
deb http://httpredir.debian.org/debian jessie main
deb-src http://httpredir.debian.org/debian jessie main
```

Snort devrait être installé dans le dossier `/etc/snort/` (et les logs dans `/var/log/snort/`) :



The screenshot shows a terminal window with the title `root@kali: /etc/snort`. The terminal has a menu bar with `Fichier`, `Édition`, `Affichage`, `Rechercher`, `Terminal`, and `Aide`. The prompt is `root@kali:/etc/snort#`. The command `ls` has been executed, showing the following files and directories: `classification.config`, `community-sid-msg.map`, `gen-msg.map`, `reference.config`, `rules`, `snort.conf`, `snort.debian.conf`, `threshold.conf`, and `unicode.map`. The prompt is now `root@kali:/etc/snort#`.

Ce dossier contient le fichier de configuration de snort : **snort.conf** :

Vous pouvez afficher et éditer ce fichier avec la commande :

```
nano /etc/snort/snort.conf
```

Le fichier de configuration vous guide dans les étapes de configuration :

```
root@kali: ~/snort-2.9.9.0
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 2.7.4                                Fichier : etc/snort.conf

# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####

#####
# Step #1: Set the network variables.  For more information, see I
#####

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most s
ipvar EXTERNAL_NET any

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^T Orthograp.
```

Vous pouvez commencer par définir les variables **HOME\_NET** et **EXTERNAL\_NET**. Par défaut, la valeur « any » est correcte. Vous devriez cependant y placer l'adresse IP de votre machine à protéger. (La commande « **ifconfig** » vous donnera l'adresse IP en question).

Si vous avez des serveurs HTTP, FTP ou autres qui disposent d'autres adresses IP, vous pouvez les placer dans les variables concernées. Sinon elle feront référence à HOME\_NET, l'adresse de Kali. Je ne touche à rien de mon côté.

Modifiez ensuite les variables **portvar** pour correspondre aux ports utilisés par vos services. Encore une fois, la configuration par défaut est valable dans la plupart des cas.

Vous avez ensuite les **décodeurs**.

Le décodeur de paquet récupère les paquets provenant de différents types d'interfaces réseau et les prépare pour les préprocesseurs ou le moteur de détection. Les préprocesseurs servent à corriger ou interpréter des éléments avant des les envoyer au moteur de détection. Cela évite que des pirates puissent « bypasser » snort en utilisant par exemple des encodages différents pour les chaînes de caractères : « javascript » au lieu de « javascript ».

Les étapes suivantes permettent de faire des configurations plus poussées de snort, mais avant cela vous pouvez déjà essayer de le lancer avec la commande :

snort -v



```

root@kali:/etc/snort# snort -v
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

_*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.8

```

Pour quitter snort, appuyez sur CTRL + C, vous obtiendrez un aperçu de l'activité réseau qu'a étudié snort :

```

Breakdown by protocol (includes rebuilt packets):
  Eth:      81 (100.000%)
  VLAN:     0 (  0.000%)
  IP4:      69 ( 85.185%)
  Frag:     0 (  0.000%)
  ICMP:     0 (  0.000%)
  UDP:      26 ( 32.099%)
  TCP:      43 ( 53.086%)
  IP6:       2 (  2.469%)

```

## Deuxième étape : configurer snort

Snort fonctionne avec des règles (*rules*). Ces règles sont des fichiers textes qui indiquent à snort comment repérer des attaques. Vous pouvez les apercevoir dans le dossier /etc/snort/rules :



```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@kali:/etc/snort# ls rules/
attack-responses.rules      community-web-dos.rules      policy.rules
backdoor.rules              community-web-iis.rules      pop2.rules
bad-traffic.rules           community-web-misc.rules     pop3.rules
chat.rules                  community-web-php.rules      porn.rules
community-bot.rules         ddos.rules                   rpc.rules
community-deleted.rules     deleted.rules                 rservices.rules
community-dos.rules         dns.rules                    scan.rules
community-exploit.rules     dos.rules                    shellcode.rules
community-ftp.rules         experimental.rules           smtp.rules
community-game.rules        exploit.rules                 snmp.rules
community-icmp.rules        finger.rules                  sql.rules
community-imap.rules        ftp.rules                     telnet.rules
community-inappropriate.rules icmp-info.rules              tftp.rules
community-mail-client.rules icmp.rules                    virus.rules
community-misc.rules        imap.rules                    web-attacks.rules
community-nntp.rules        info.rules                    web-cgi.rules
community-oracle.rules      local.rules                   web-client.rules
community-policy.rules      misc.rules                    web-coldfusion.rules
community-sip.rules         multimedia.rules              web-front.rules
```

Nous nous baserons sur la capture d'écran ci-dessous à des fins de compatibilité. Cela dit, snort uniformise ses règles et il est donc tout à fait possible que vous n'ayez pas autant de règles dans le dossier rules. Par ailleurs, en utilisant PulledPork, vous n'avez qu'à définir vos propres règles dans le fichier local.rules, les autres seront automatiquement téléchargées et utilisées via snort et ses partenaires.

Voici par exemple les règles de community-sql-injection.rules :

```
GNU nano 2.7.4      Fichier : rules/community-sql-injection.rules
# Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# These rules are licensed under the GNU General Public License.
# Please see the file LICENSE in this directory for more details.
# $Id: community-sql-injection.rules,v 1.10 2006/10/19 20:19:34 a
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"COMMUN
$CustomSearchField.asp\x3F[^\r\n]*exec/Ui"; classtype:web-applica
```

Snort va détecter des URL suspectes (que les attaquants vont tester pour entrer dans un site) et lancer l'alerte.

Les règles sont régulièrement mises à jour, c'est pour cela que vous propose de vous inscrire sur la page d'accueil de snort.org (vous devez le faire pour utiliser PulledPork). L'idée est de mettre à jour régulièrement les règles, tout comme l'on met à jour notre antivirus.

Vous pouvez bien sûr créer vos propres règles. Le fichier **local.rules** du dossier rules est prévu pour

cela.

Vous pouvez l'éditer et y ajouter une règle pour tester snort (la règle doit être sur une ligne) :

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1;
sid:10000001; rev:001; classtype:icmp-event;)
```

```
GNU nano 2.7.4                                Fichier : 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
# additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1;
sid:10000001; rev:001; classtype:icmp-event;)
```

L'ajout d'une règle se fait en lui précisant son identifiant unique « sid », un message « msg », un « classtype » selon ce qui est disponible dans le fichier classification.config.

Testons la configuration de snort avec la commande suivante :

```
sudo snort -T -i eth0 -c /etc/snort/snort.conf
```

```
4151 Snort rules read
 3477 detection rules
   0 decoder rules
   0 preprocessor rules
3477 Option Chains linked into 271 Chain Headers
 0 Dynamic rules
+++++
```

Lançons snort pour tester notre règle :

```
sudo snort -A console -q -u root -g root -c /etc/snort/snort.conf -i eth0
```

-console : signifie que l'on affiche les résultats dans la console.

-q : signifie mode silencieux et nous épargne les affichages de bannières...etc.

-c <chemin> : le chemin vers le fichier de config

-i <interface> : l'interface réseau cible

-u et -g : utilisateur et groupe avec lesquels lancer snort.

À noter qu'il est recommandé de ne pas lancer snort en tant que root :

```
sudo groupadd snort
```

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

Donnez ensuite les bons droits aux répertoires de snort :

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

Vous pourrez lancer la commande avec :

```
sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
```

Le ping icmp est détecté avec succès en utilisant Metasploitable pour tester.  
Et un scan nmap est naturellement détecté lui-aussi :



```

n: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.39 -> 192.168.1.12
7/27-16:35:01.432928  [**] [1:408:5] ICMP Echo Reply [**] [Classification:
activity] [Priority: 3] {ICMP} 192.168.1.39 -> 192.168.1.12
7/27-16:35:01.460616  [**] [1:10000001:1] ICMP test detected [**]
n: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.12 -> 192.168.1.39
7/27-16:35:01.460616  [**] [1:384:5] ICMP PING [**] [Classification:
ty] [Priority: 3] {ICMP} 192.168.1.12 -> 192.168.1.39
7/27-16:35:01.461617  [**] [1:10000001:1] ICMP test detected [**]
n: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.39 -> 192.168.1.12
7/27-16:35:01.461617  [**] [1:408:5] ICMP Echo Reply [**] [Classification:
activity] [Priority: 3] {ICMP} 192.168.1.39 -> 192.168.1.12
7/27-16:35:01.701512  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification:
pted Information Leak] [Priority: 2] {TCP} 192.168.1.12:54820 -> 192.168.1.
948
7/27-16:35:01.911722  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification:
pted Information Leak] [Priority: 2] {TCP} 192.168.1.12:54820 -> 192.168.1.
948
7/27-16:35:02.121752  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification:
pted Information Leak] [Priority: 2] {TCP} 192.168.1.12:54820 -> 192.168.1.
948
pt  Metasploitable [En fonction] - Oracle VM VirtualBox
94  Fichier Machine Écran Entrée Périphériques Aide
7/  root@metasploitable:~# nmap -O 192.168.1.39
pt
94 Starting Nmap 4.53 ( http://insecure.org ) at 2017-02-02 18:27 EST

```

Vous pouvez appuyer sur CTRL + C pour quitter snort.

### Installer Snort en tant que Système de Prévention d'Intrusions

Snort peut être installé et utilisé selon deux modes : Système de **Détection** d'Intrusions (IDS), et système de **Prévention** d'Intrusions (IPS).

Jusqu'ici nous avons parlé du premier mode. Le deuxième mode semble à première vue préférable car il permet de bloquer dynamiquement des machines qui génèrent des alertes.

Il y a cependant une mise en garde à faire.

Tout d'abord, Snort peut très bien générer des **faux positifs**, c'est-à-dire lancer des alertes alors qu'aucun comportement véritablement malveillant n'a eu lieu (et cela peut concerner vos propres activités). Pour éviter cette mésaventure, il est donc nécessaire de bien préparer ses règles, et donc de ne pas utiliser toutes les règles par défaut de Snort en mode « Drop » (le mode qui va bloquer les machines générant des alertes).

Ensuite, pour installer Snort en mode IPS, il faut posséder d'**au moins 3 cartes réseaux** sur votre machine. Snort, dans le mode IPS, crée un pont transparent entre deux segments réseaux. Cela signifie que Snort a deux interfaces réseaux (sans adresses IP et en mode promiscuité). Snort va ensuite écouter le trafic sur les deux interfaces, et lorsqu'un paquet arrive sur l'une d'elles, les données seront inspectées et les règles appliquées. Snort décide de refuser le paquet, ou de l'autoriser et l'envoyer sur l'autre interface sans modifications.

La troisième interface est l'interface réseau habituelle de la machine (avec une adresse IP), qui servira à administrer Snort.

Pour configurer les deux interfaces que Snort doit utiliser, vous pouvez éditer le fichier interfaces :

sudo nano /etc/network/interfaces

Et voici un exemple de configuration (à adapter) :

```
# Administrative interface
auto eth0
iface eth0 inet dhcp
# Première interface par pont
auto eth1
iface eth1 inet manual
    up ifconfig $IFACE 0.0.0.0 up
    up ip link set $IFACE promisc on
    post-up ethtool -K $IFACE gro off
    post-up ethtool -K $IFACE lro off
    down ip link set $IFACE promisc off
    down ifconfig $IFACE down
# Deuxième interface par pont
auto eth2
iface eth2 inet manual
    up ifconfig $IFACE 0.0.0.0 up
    up ip link set $IFACE promisc on
    post-up ethtool -K $IFACE gro off
    post-up ethtool -K $IFACE lro off
    down ip link set $IFACE promisc off
    down ifconfig $IFACE down
```

Vous pouvez ensuite éditer le fichier de configuration **/etc/snort/snort.conf** pour activer DAQ en ajoutant les lignes suivantes (la configuration DAG se situe vers le début du fichier de configuration) :

config daq: afpacket config daq\_mode: inline

Le mode inline de Snort (IPS) est ainsi activé. On teste la configuration avec :

sudo snort -T -c /etc/snort/snort.conf -Q -i eth1:eth2 Et si tout est ok, on peut lancer Snort en mode inline :

sudo /usr/local/bin/snort -A console -Q -c /etc/snort/snort.conf -i eth1:eth2 -N

EDIT: Si vous avez l'erreur « **»ERROR: Can't initialize DAQ afpacket (-1) – create\_instance: Could not find index for device eth1 Fatal Error, Quitting...** » », Thibault, membre du cours, indique que les deux précédentes commandes doivent être légèrement modifiées si cela ne fonctionne pas chez vous, voici ce qu'il propose:

sudo snort -T -c /etc/snort/snort.conf -i eth1:eth2

en enlevant donc l'option -Q.

et

sudo snort -T -c /usr/local/bin/snort -A console -c /etc/snort/snort.conf -i eth1:eth2 -N

en ajoutant -T -c.

Les commandes citées dans ce document pouvant varier suivant la version de Snort que vous possédez.

Voir aussi (pour l'erreur DAQ afpacket) : <https://www.linuxquestions.org/questions/linux-newbie-8/snort-error-can%27t-start-daq-1-socket-operation-not-permitted-4175480943/>

Vos règles doivent ensuite être adaptées en conséquence (placez « drop » à la place de « alert » aux règles dont vous voulez bloquer les machines au lieu de lancer une simple alerte).

Votre aventure avec snort commence seulement, il y a encore beaucoup de choses à connaître, mais vous savez à présent comment utiliser snort de façon basique.

Je vous propose de lire la documentation si vous souhaitez en savoir plus :



Comment créer des règles :

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html>

Documentation complète : <https://www.snort.org/#documents>