

# **GUIDE D'INSTALLATION DE SNORT SOUS LINUX**

Cycle : ING2

Auteur :

- Josué DA-MATHA
- Khorem KANHO
- Imtynane ODJO



## Table des matières

<b>1. Installation de SNORT sur Kali .....</b>	<b>3</b>
1.1. Backup Kali's source.list .....	3
1.2. Remove update.....	3
1.3. Change source.list content.....	3
1.4. Add the specified public keys .....	4
1.5. Update .....	4
1.6. Install SNORT .....	5
<b>2. Prise en mains de SNORT .....</b>	<b>6</b>
2.1. Vérification de la version de SNORT .....	6
2.2. Visualiser le contenu du fichier snort.conf .....	6
2.3. Trouver l'adresse ip de ma machine .....	7
2.4. Tester la configuration de SNORT .....	7
2.5. Obtention des informations sur les hôtes et services .....	8
2.6. Lancement de SNORT en mode console.....	8



## 1. Installation de SNORT sur Kali

### 1.1. Backup Kali's source.list

```
# mv /etc/apt/sources.list /etc/apt/sources.list.bak
```

```
(root@kali)~# mv /etc/apt/sources.list /etc/apt/sources.list.bak
```

### 1.2. Remove update

```
# find /var/lib/apt/lists -type f -exec rm {} \;
```

```
(root@kali)~# find /var/lib/apt/lists -type f -exec rm {} \;
```

### 1.3. Change source.list content

```
# sudo nano /etc/apt/sources.list
```

```
(root@kali)~# sudo nano /etc/apt/sources.list
```

**Après avoir taper cette commande, vous allez copier ce bout de code :**

```
deb [arch=arm64] http://ports.ubuntu.com/ubuntu-ports focal main restricted universe multiverse
deb [arch=arm64] http://ports.ubuntu.com/ubuntu-ports focal-updates main restricted universe multiverse
deb [arch=arm64] http://ports.ubuntu.com/ubuntu-ports focal-security main restricted universe multiverse
deb [arch=i386,amd64] http://us.archive.ubuntu.com/ubuntu/ focal main restricted universe multiverse
deb [arch=i386,amd64] http://us.archive.ubuntu.com/ubuntu/ focal-updates main restricted universe multiverse
deb [arch=i386,amd64] http://security.ubuntu.com/ubuntu focal-security main restricted universe multiverse
```

**Et puis enfin sauvegarder.**

## 1.4. Add the specified public keys

```
# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32
```

```
(root@kali)-[~]
# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead
(see apt-key(8)).
Executing: /tmp/apt-key-gpghome.WanpsL0bCn/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32
gpg: key 3B4FE6ACC0B21F32: public key "Ubuntu Archive Automatic Signing Key (
2012) <ftpmaster@ubuntu.com>" imported
gpg: Total number processed: 1
gpg:          imported: 1
```

```
# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C
```

```
(root@kali)-[~]
# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead
(see apt-key(8)).
Executing: /tmp/apt-key-gpghome.KC2ZlDl1Uu/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C
gpg: key 871920D1991BC93C: public key "Ubuntu Archive Automatic Signing Key (
2018) <ftpmaster@ubuntu.com>" imported
gpg: Total number processed: 1
gpg:          imported: 1
```

## 1.5. Update

```
# sudo apt update
```

```
(root@kali)-[~]
# sudo apt update
Get:1 http://ports.ubuntu.com/ubuntu-ports focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports focal-updates InRelease [114 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports focal-security InRelease [114 kB]
```

Dès que vous taper la commande **apt update**, cela peut prendre du temps ; ne paniquez pas c'est normal. Patientez seulement.



## # sudo apt install

```
(root@kali)-[~]  
# sudo apt install  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
0 upgraded, 0 newly installed, 0 to remove and 51 not upgraded.
```

## 1.6. Install SNORT

### # sudo apt install snort

```
(root@kali)-[~]  
# sudo apt install snort  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libdaq2 libestr0 libfastjson4 oinkmaster rsyslog snort-common  
  snort-common-libraries snort-rules-default  
Suggested packages:  
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl  
  | rsyslog-gnutls rsyslog-gssapi rsyslog-relp snort-doc
```

## 2. Prise en mains de SNORT

### 2.1. Vérification de la version de SNORT

#snort version

```
(root@kali)-[/home/kali]
# snort --version

--> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 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
```

### 2.2. Visualiser le contenu du fichier snort.conf

#cat /etc/snort/snort.conf

```
(root@kali)-[/home/kali]
# cat /etc/snort/snort.conf

# VRT Rule Packages Snort.conf
#
# For more information visit us at:
#   http://www.snort.org           Snort Website
#   http://vrt-blog.snort.org/     Sourcefire VRT Blog
#
# Mailing list Contact:  snort-sigs@lists.sourceforge.net
# False Positive reports: fp@sourcefire.com
# Snort bugs:           bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.7.0
#
# Snort build options:
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-flexresp3
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder.
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
```



## # ifconfig

## 2.4. Tester la configuration de SNORT

-l **eth0**: Indique l'interface réseau à surveiller, dans ce cas, "eth0".

```
(root@kali)~# snort -T -c /etc/snort/snort.conf -i eth0
Running in Test mode

--= Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
```





### Bon à savoir :

Au lieu d'entrer l'adresse ip, nous avons utilisé directement l'interface réseau où se situe l'adresse ip. Dès que vous avez ce message : **Snort successfully validated the configuration ! Snort exiting.** Là vous avez réussi sinon reprenez !!

```
Snort successfully validated the configuration!  
Snort exiting
```

```
(root@kali)-[/home/kali]  
#
```

## 2.5. Obtention des informations sur les hôtes et services

Ensuite, vous vous connectez en tant qu'admin sur une autre fenêtre pour faire la commande nmap

# nmap @ip

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nmap 192.168.11.133  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 06:22 EDT  
Nmap scan report for 192.168.11.133 (192.168.11.133)  
Host is up (0.0000080s latency).  
All 1000 scanned ports on 192.168.11.133 (192.168.11.133) are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

## 2.6. Lancement de SNORT en mode console

# snort -A Console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

```
(root@kali)-[/home/kali]  
# snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0  
03/27-06:18:21.032237  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.11.1:52426 → 239.255.255.250:1900
```





- **-A Console:** Cette option spécifie le mode de sortie des alertes générées par Snort. Dans ce cas, les alertes seront affichées dans la console.
- **-q:** Cette option spécifie un mode silencieux où les messages de démarrage et d'arrêt de Snort sont désactivés. Il ne produira que des alertes en sortie.
- **-u snort:** Cette option spécifie l'utilisateur sous lequel Snort s'exécutera. Dans ce cas, Snort s'exécutera sous l'utilisateur "snort".
- **-g snort:** Cette option spécifie le groupe sous lequel Snort s'exécutera. Dans ce cas, Snort s'exécutera dans le groupe "snort".
- **-c /etc/snort/snort.conf:** Cette option spécifie le chemin vers le fichier de configuration de Snort à utiliser. Dans ce cas, le fichier de configuration principal est **/etc/snort/snort.conf**.
- **-i eth0:** Cette option spécifie l'interface réseau sur laquelle Snort effectuera la surveillance du trafic. Dans cet exemple, Snort surveillera l'interface "eth0".