Ecole Centrale Polytechnique d'Ingénieurs

GUIDE D'INSTALLATION DE SNORT SOUS LINUX

Cycle : ING2

Auteur :

- Josué DA-MATHA
- Khorem KANHO
- Imtynane ODJO

Année Académique : 2023 -2024

Table des matières

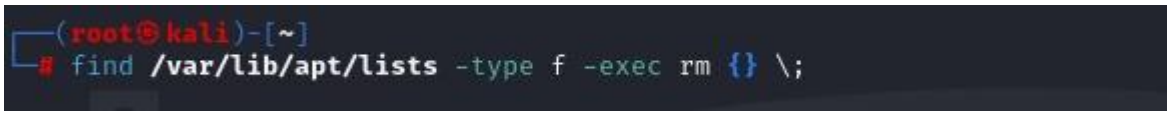
1. Installation de SNORT sur Kali

1.1. Backup Kali's source.list

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

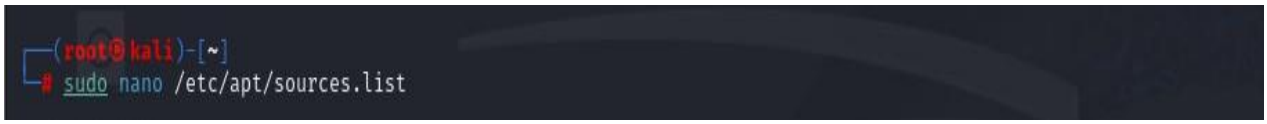
1.2. Remove update

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



1.3. Change source.list content

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 3B4FE6ACC0B
21F32
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.ubu
ntu.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 871920D1991
BC93C
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.ubu
ntu.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

1.6. Install SNORT

 # sudo apt install snort

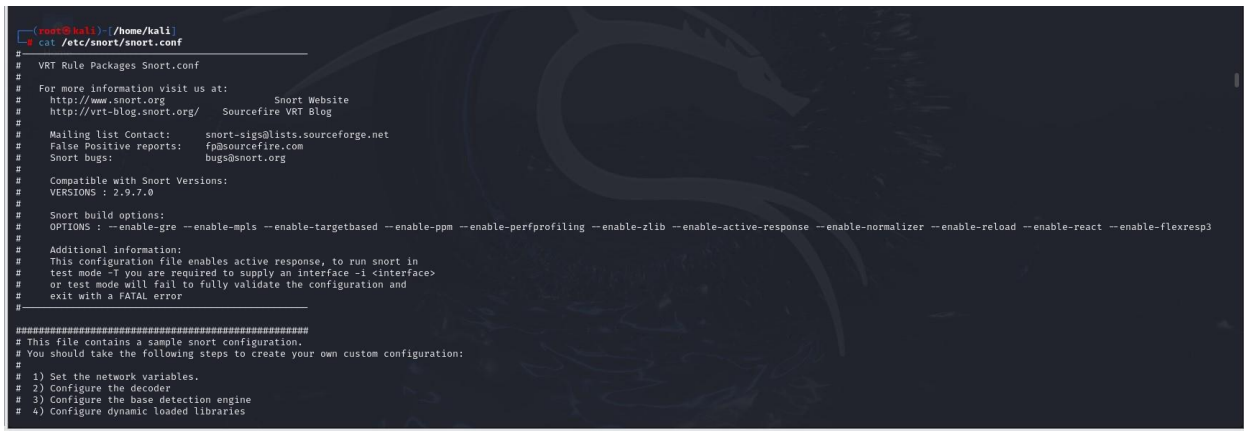
2. Prise en mains de SNORT

2.1. Vérification de la version de SNORT

#snort version

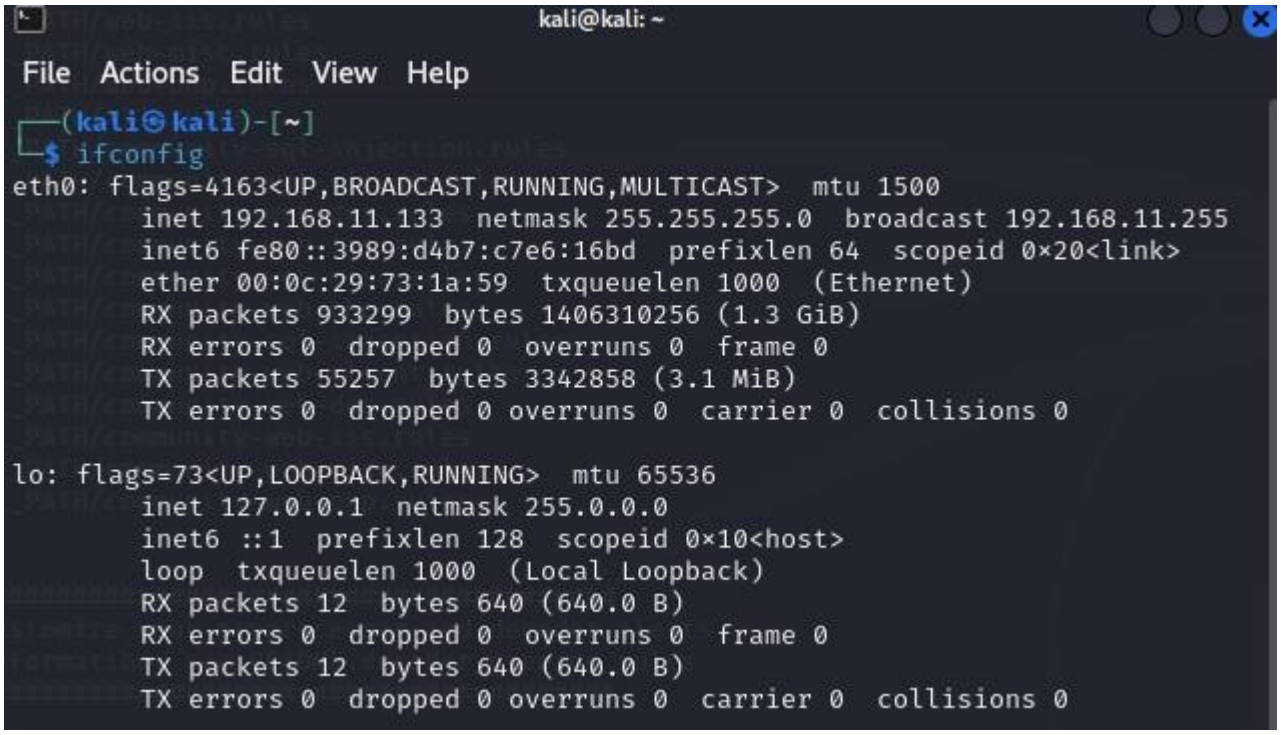
2.2. Visualiser le contenu du fichier snort.conf

#cat /etc/snort/snort.conf



2.3. Trouver l'adresse ip de ma machine

 # ifconfig



2.4. Tester la configuration de SNORT

Snort -T -C /etc/snort/snort.conf -I eth0

-T: Cela indique à Snort de tester la configuration sans démarrer la surveillance active.

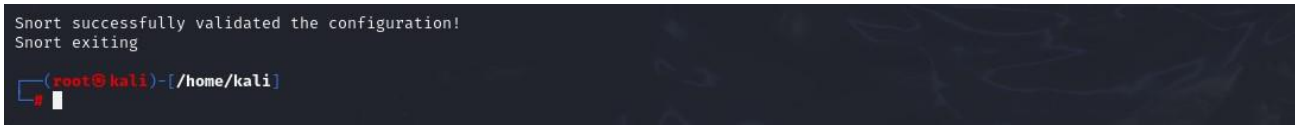
-C /etc/snort/snort.conf: Spécifie le chemin du fichier de configuration principal de Snort.

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

Bon à savoir :

Au lieu d'entrer l'adresse ip, nous avons utilisé directement l'interface réseau où se situe l'adresse ip.

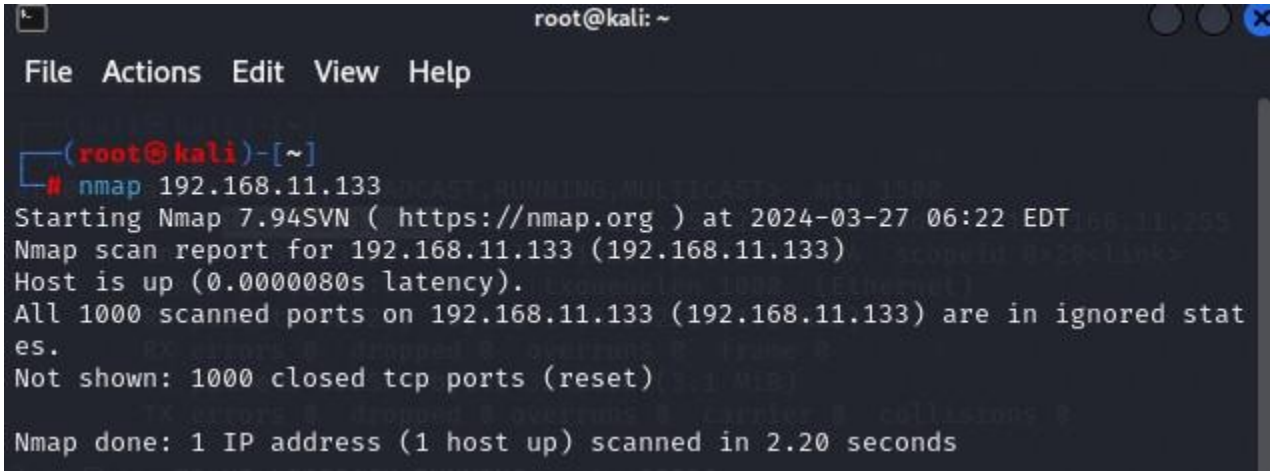
Dès que vous avez ce message : **Snort successfully validated the configuration ! Snort exiting**. Là vous avez réussir sinon reprenez !!



2.5. Obtention des informations sur les hôtes et services

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

 # nmap @ip



2.6. Lancement de SNORT en mode console

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

- **-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".

