

---

# Suricata Partie 1: IDS/IPS (Installation, configuration et simulation)

## Table des matières :

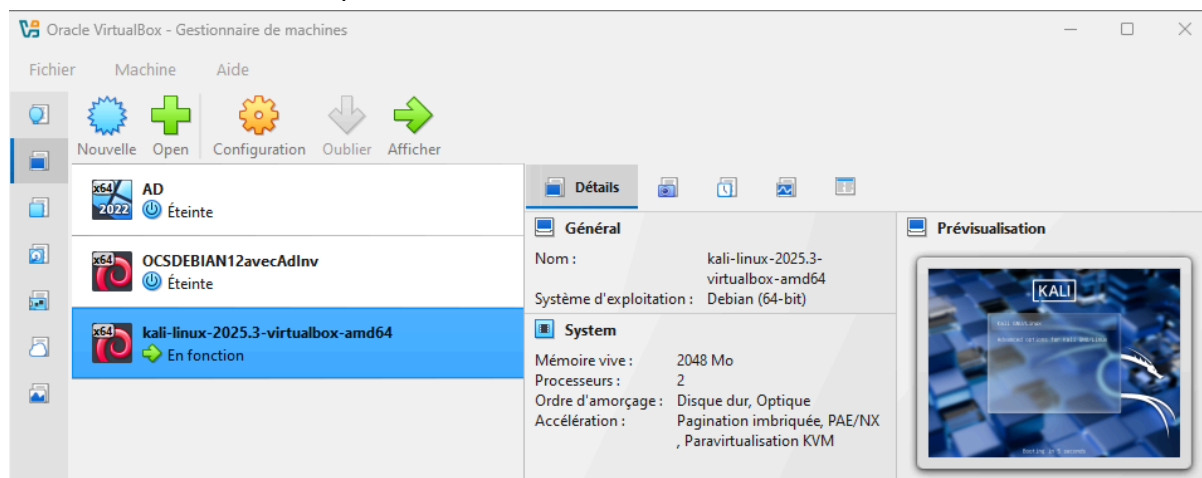
<b>1. Travail à faire.....</b>	<b>2</b>
<b>1) Configuration de la machine Kali 2025 :.....</b>	<b>3</b>
<b>2) VM Suricata : installer Suricata et jq (json query).....</b>	<b>16</b>
<b>3) Modification du fichier de configuration /etc/suricata/suricata.yaml :.....</b>	<b>18</b>
<b>4) Importer les règles Emerging Threat Open.....</b>	<b>21</b>
<b>5) Test du bon fonctionnement en mode IDS de Suricata (détection trafic suspect) ..</b>	<b>23</b>
<b>6) Créer 2 règles personnalisées :.....</b>	<b>25</b>
<b>7) Basculer Suricata en mode IPS :.....</b>	<b>30</b>
a) Configuration de Suricata :.....	30
b) Configurer IPTables (NFQUEUE).....	32
<b>8) Test du bon fonctionnement du mode IPS :.....</b>	<b>33</b>
<b>9) Créer une règle permettant de bloquer une attaque DOS (SYN Flood) sans bloquer les requêtes http légitimes :.....</b>	<b>36</b>

## 1. Travail à faire.

1. Configurer Kali 2025 ;
2. Installation de Suricata, du serveur SSH et du serveur Web sur la VM Suricata ;
3. Configurer Suricata ;
4. Importer l'ensemble des règles ET Open (fichier suricata.rules) ;
5. Tester le bon fonctionnement de Suricata en tant que HIDS (cf. commande curl et la règle sid 2100498 ainsi que les logs fast.log et eve.json) ;
6. Créer 2 règles personnalisées (fichier custom.rules) déclenchant une alerte (ICMP et SSH).  
Tester et vérifiez les 2 logs ;
7. Configurer Suricata en tant que HIPS (utiliser le FW netfilter IPTables).
8. Remplacer l'action Alert par Drop dans la règle avec le sid 2100498 puis tester avec la commande curl. Par ailleurs, les pings doivent dorénavant être supprimés.
9. Lire attentivement les échanges entre Victor Julien et Nurchaliza. Créer une règle permettant de bloquer une attaque DOS (SYN Flood) sans bloquer les requêtes http légitimes. Tester avec l'outil Hping3 (réaliser une capture de trames : segments SYN).
10. Installer Suricata sur la VM pfSense. Configurer Suricata en tant que NIPS (le mode IPS activé sur l'interface WAN). Lancer, à l'aide de hping3, une attaque DOS depuis la machine Kali en accès pont déplacée côté WAN.

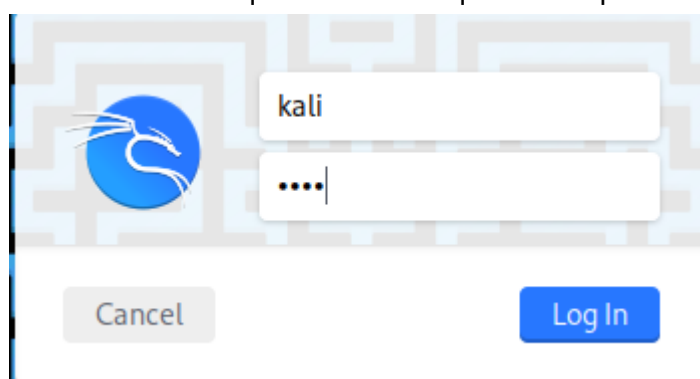
# 1) Configuration de la machine Kali 2025 :

La VM kalilinux a été récupérée



Utilisateur : kali ; Mot de passe : kali

Nous saisissons kqli sur le clavier que ce soit pour l'utilisateur et le mot de passe

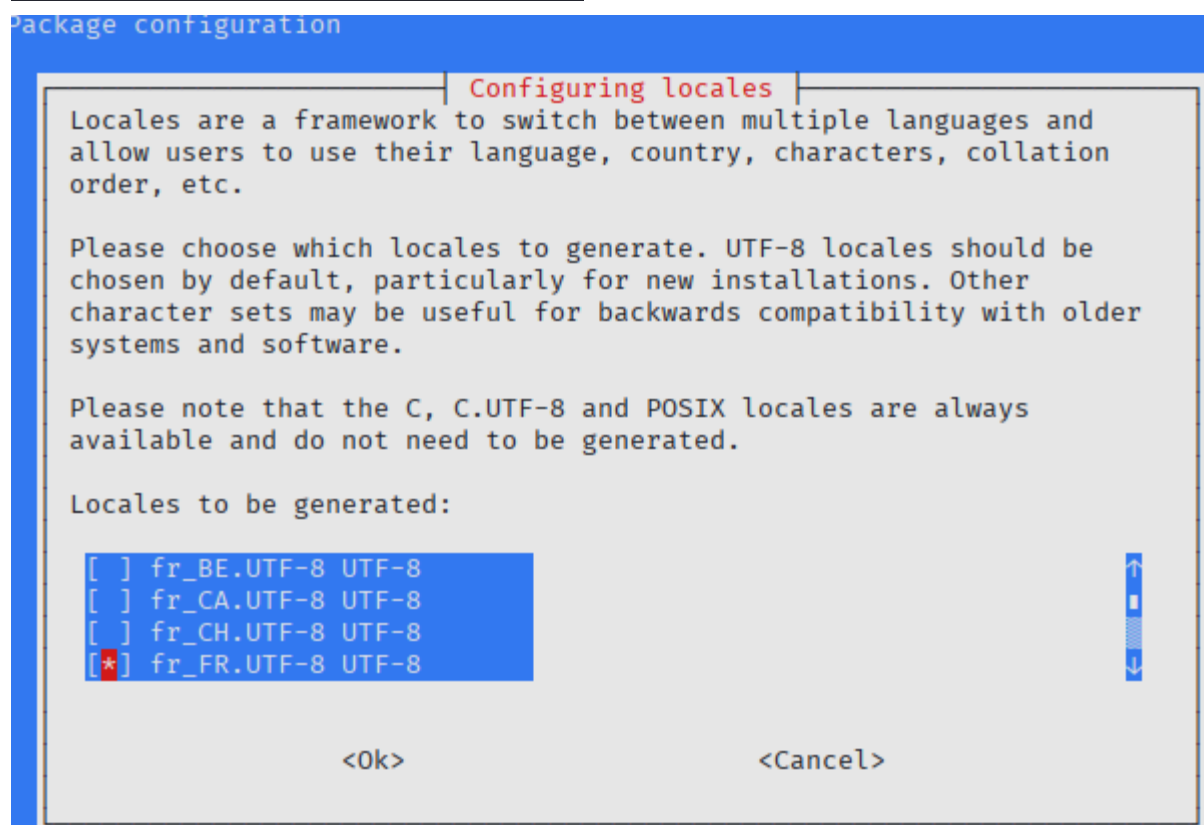


Les additions invités sont déjà ajoutées à la VM.

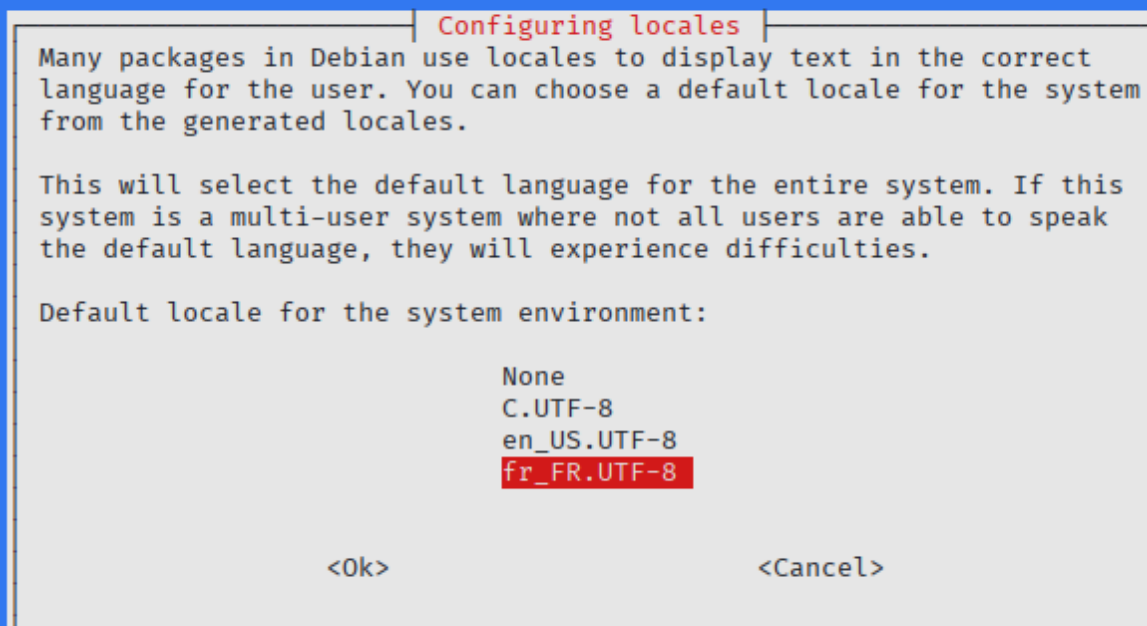


- Nous allons mettre l'interface graphique en Français :

```
(kali㉿kali)-[~]  
└─$ sudo dpkg-reconfigure locales  
[sudo] password for kali:
```

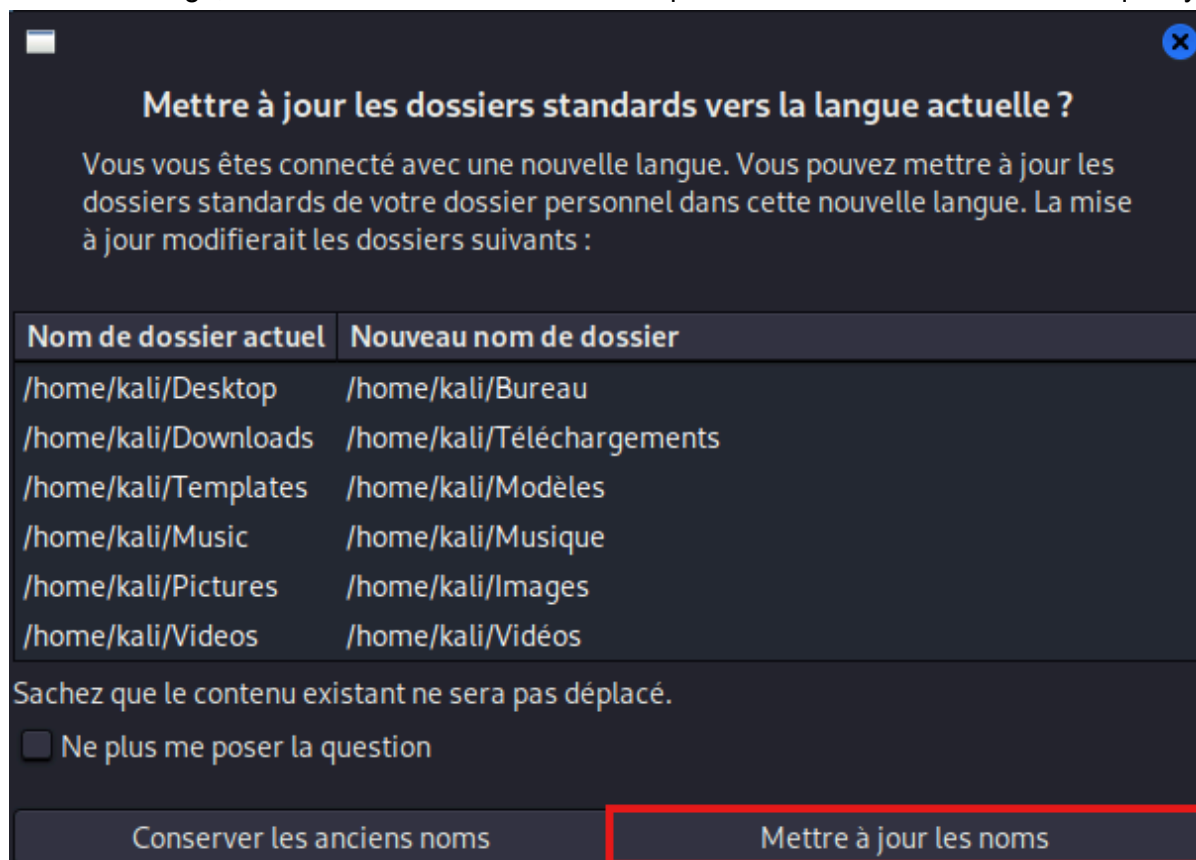


## Package configuration



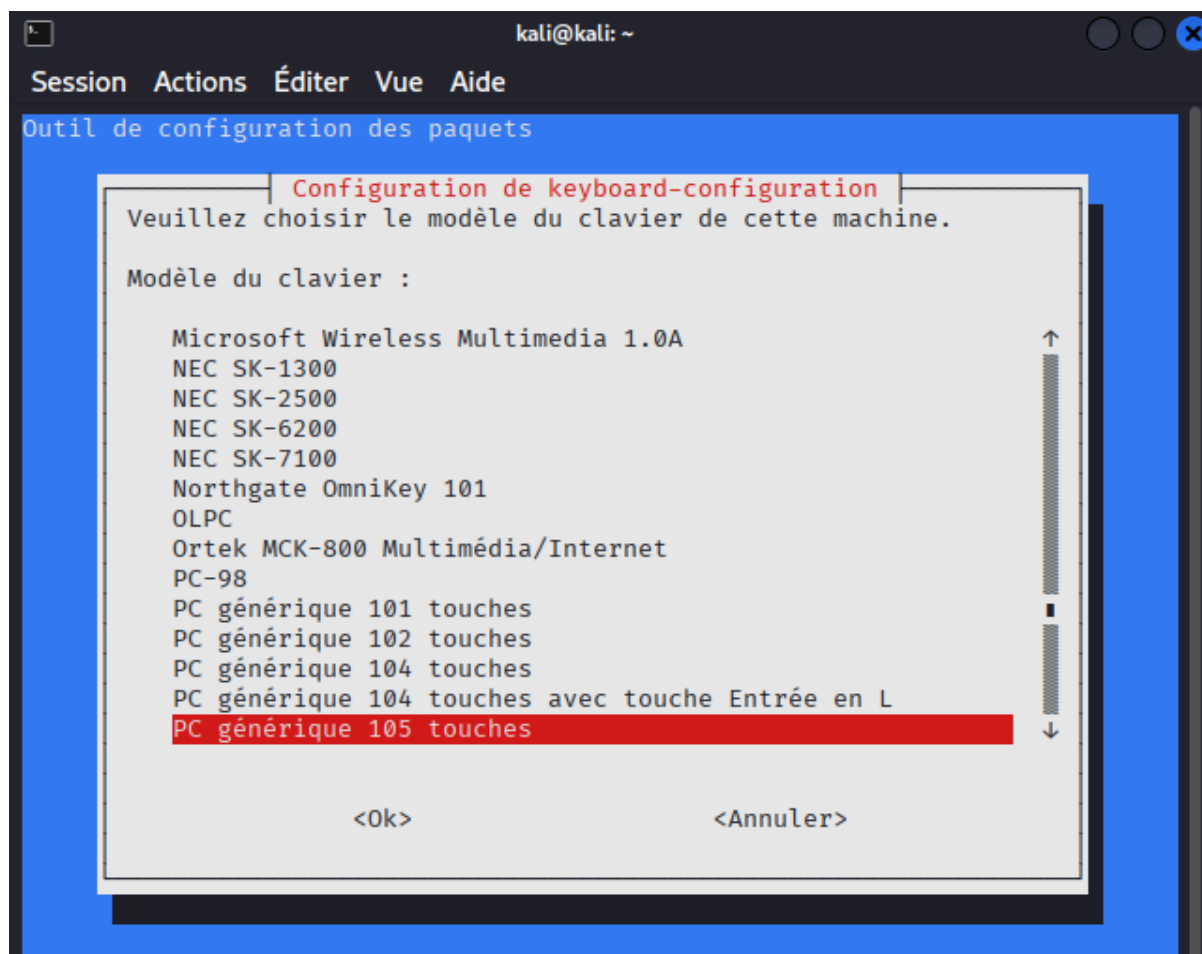
```
(kali㉿kali)-[~]
└─$ sudo dpkg-reconfigure locales
Generating locales (this might take a while)...
 en_US.UTF-8 ... done
 fr_FR.UTF-8 ... done
Generation complete.
```

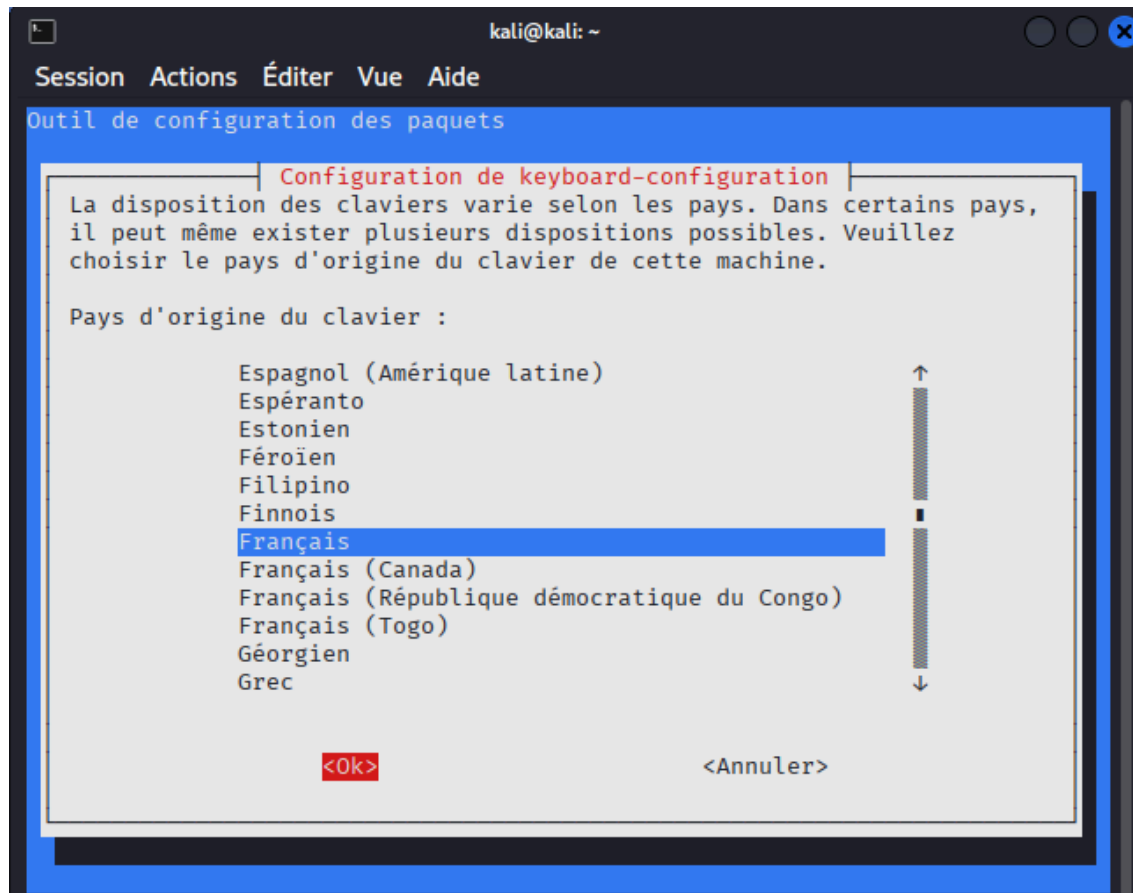
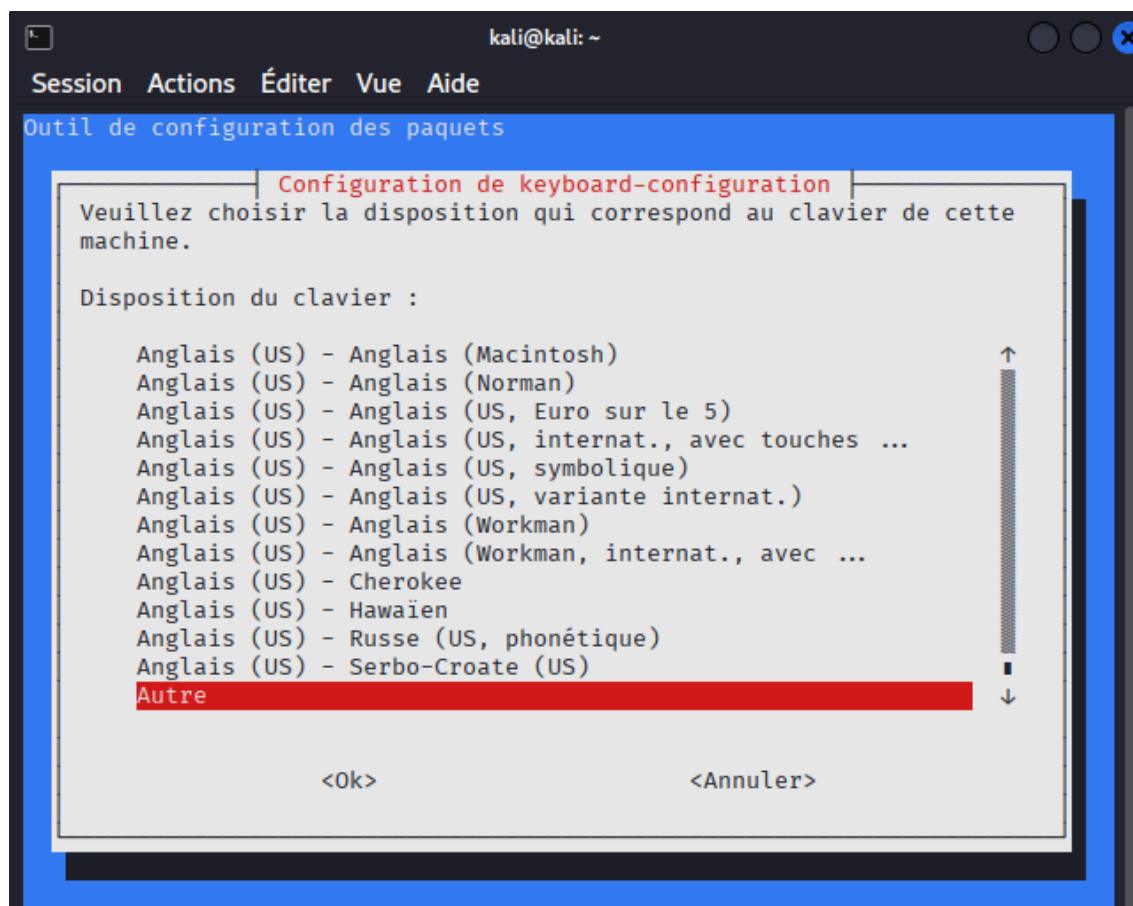
Au redémarrage, nous devons saisir de nouveau kqli comme le clavier est encore en qwerty.

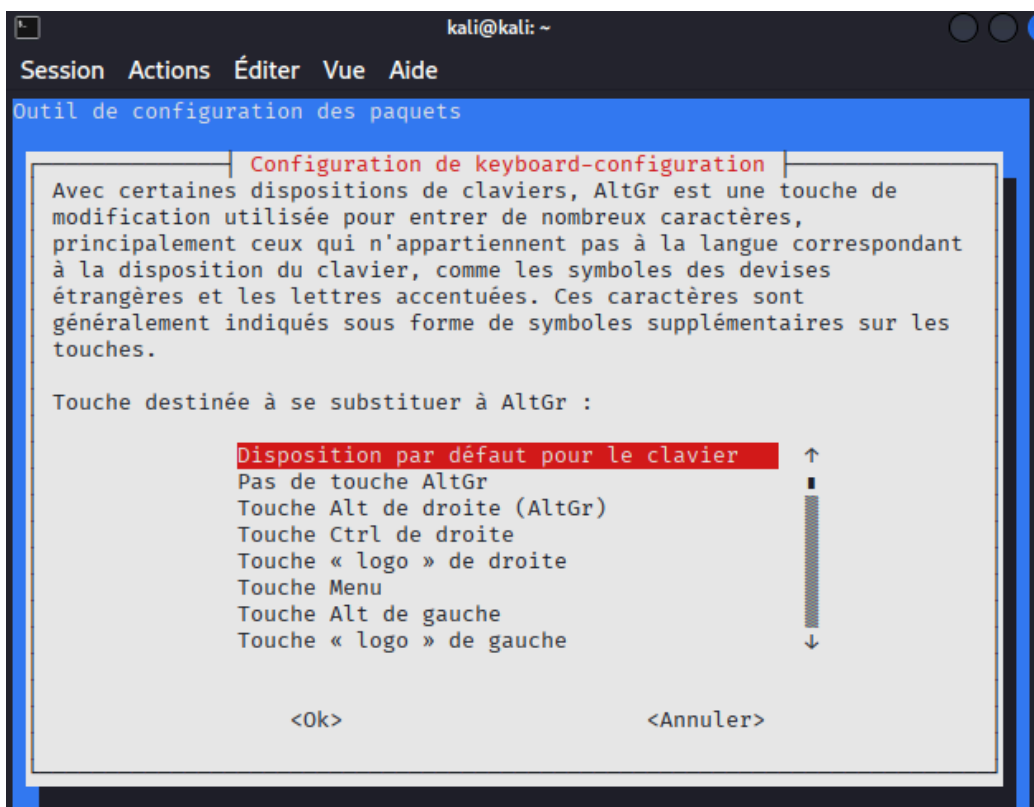
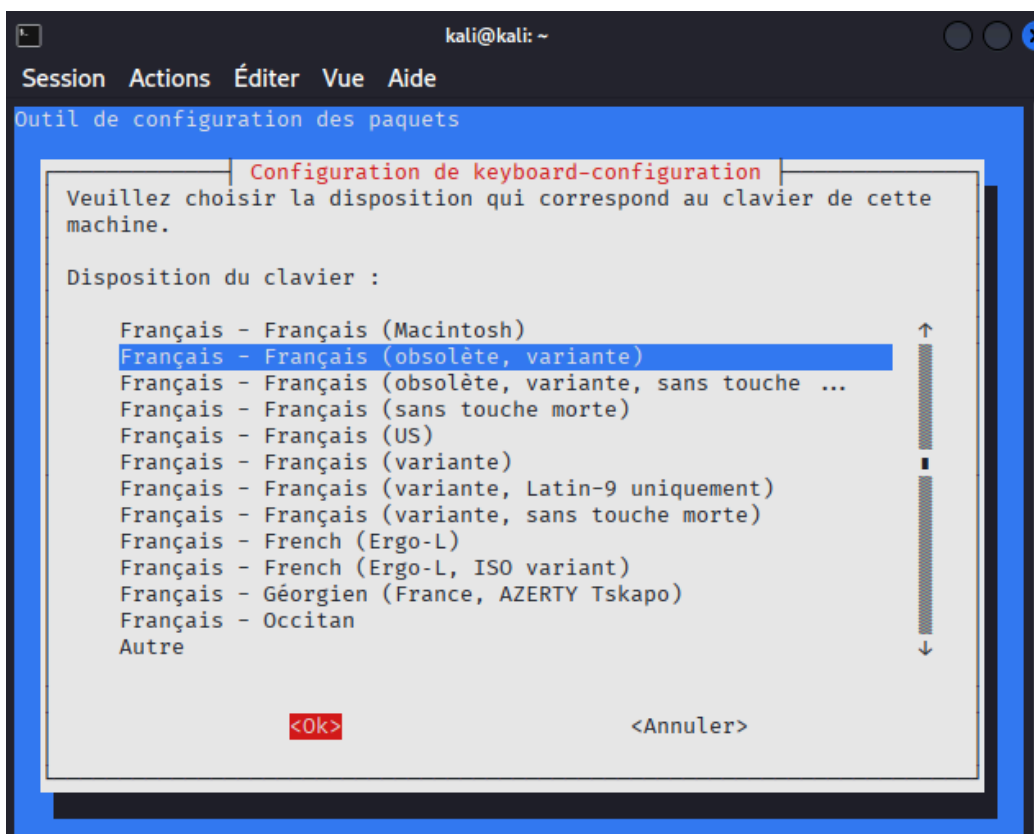


▪ Nous allons mettre le clavier en Français :

```
kali@kali: ~  
Session Actions Éditer Vue Aide  
└─(kali@kali)-[~]  
└─$ sudo dpkg-reconfigure keyboard6configuration  
[sudo] Mot de passe de kali :  
dpkg-query: le paquet « keyboard6configuration » n'est pas installé et aucune  
information n'est disponible  
Utilisez dpkg --info (= dpkg-deb --info) pour examiner les fichiers d'archive  
./usr/sbin/dpkg-reconfigure: keyboard6configuration n'est pas installé  
└─(kali@kali)-[~]  
└─$ sudo dpkg-reconfigure keyboard-configuration
```





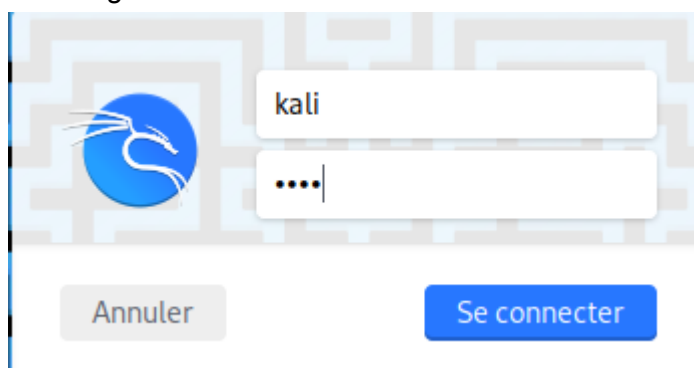




- Nous procédons par un redémarrage de la VM

```
kali@kali: ~  
Session Actions Éditer Vue Aide  
(kali@kali)-[~]  
└─$ sudo dpkg-reconfigure keyboard6configuration  
[sudo] Mot de passe de kali :  
dpkg-query: le paquet « keyboard6configuration » n'est pas installé et aucune  
information n'est disponible  
Utilisez dpkg --info (= dpkg-deb --info) pour examiner les fichiers d'archive  
./usr/sbin/dpkg-reconfigure: keyboard6configuration n'est pas installé  
(kali@kali)-[~]  
└─$ sudo dpkg-reconfigure keyboard-configuration  
(kali@kali)-[~]  
└─$ reboot
```

- Nous lançons la machine kaili normalement  
La configuration du clavier a été réalisée avec succès



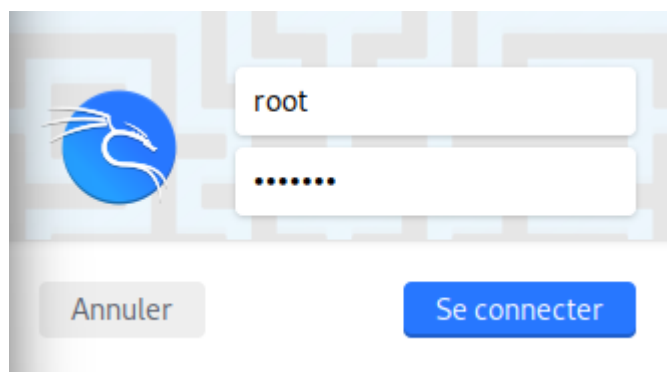
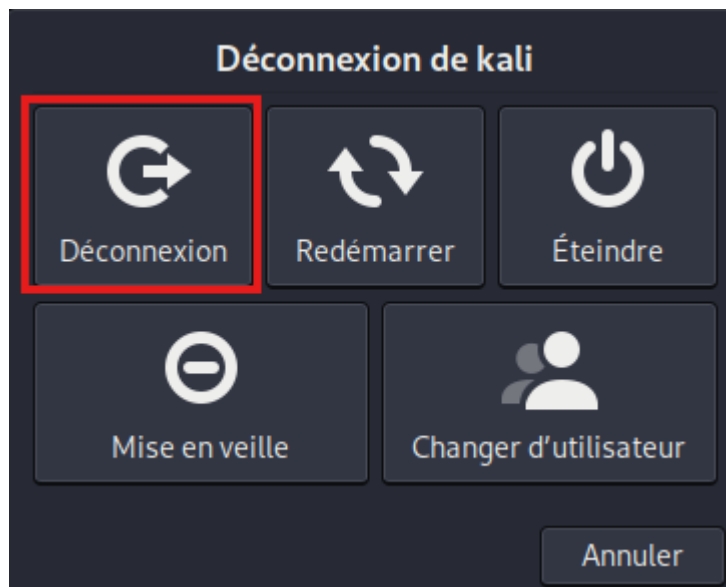
- Nous allons activer le compte root :  
Tout d'abord nous allons procéder par un (apt-get update avant)

```
(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] Mot de passe de kali :
Réception de : 1 http://archive-4.kali.org/kali kali-rolling InRelease [34,0
kB]
Réception de : 2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packa
ges [20,9 MB]
Réception de : 3 http://archive-4.kali.org/kali kali-rolling/main amd64 Conte
nts (deb) [51,8 MB]
Réception de : 4 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Pa
ckages [115 kB]
Réception de : 5 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Co
ntents (deb) [258 kB]
Réception de : 6 http://archive-4.kali.org/kali kali-rolling/non-free amd64 P
ackages [187 kB]
Réception de : 7 http://archive-4.kali.org/kali kali-rolling/non-free amd64 C
ontents (deb) [891 kB]
Réception de : 8 http://archive-4.kali.org/kali kali-rolling/non-free-firmwar
e amd64 Packages [11,3 kB]
Réception de : 9 http://archive-4.kali.org/kali kali-rolling/non-free-firmwar
e amd64 Contents (deb) [28,4 kB]
74,2 Mo réceptionnés en 15s (4 878 ko/s)
```

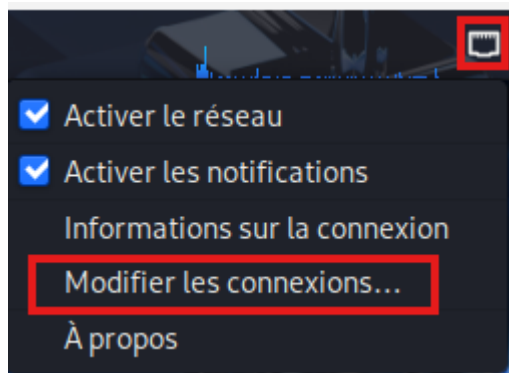
```
(kali㉿kali)-[~]
└─$ sudo apt-get install kali-root-login
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
 kali-root-login
0 mis à jour, 1 nouvellement installés, 0 à enlever et 808 non mis à jour.
Il est nécessaire de prendre 6 776 B dans les archives.
Après cette opération, 33,8 ko d'espace disque supplémentaires seront utilisé
s.
Ign : 1 http://mirror.es.cdn-perfprod.com/kali kali-rolling/main amd64 kali-r
oot-login all 2019.4.0
Réception de : 1 http://mirror.es.cdn-perfprod.com/kali kali-rolling/main amd
64 kali-root-login all 2019.4.0 [6 776 B]
6 776 o réceptionnés en 21s (316 o/s)
Sélection du paquet kali-root-login précédemment désélectionné.
(Lecture de la base de données... 417218 fichiers et répertoires déjà install
és.)
Préparation du dépaquetage de .../kali-root-login_2019.4.0_all.deb ...
Ajout de « détournement de /etc/gdm3/daemon.conf en /etc/gdm3/daemon.conf.ori
```

Mot de passe de root : Azerty0

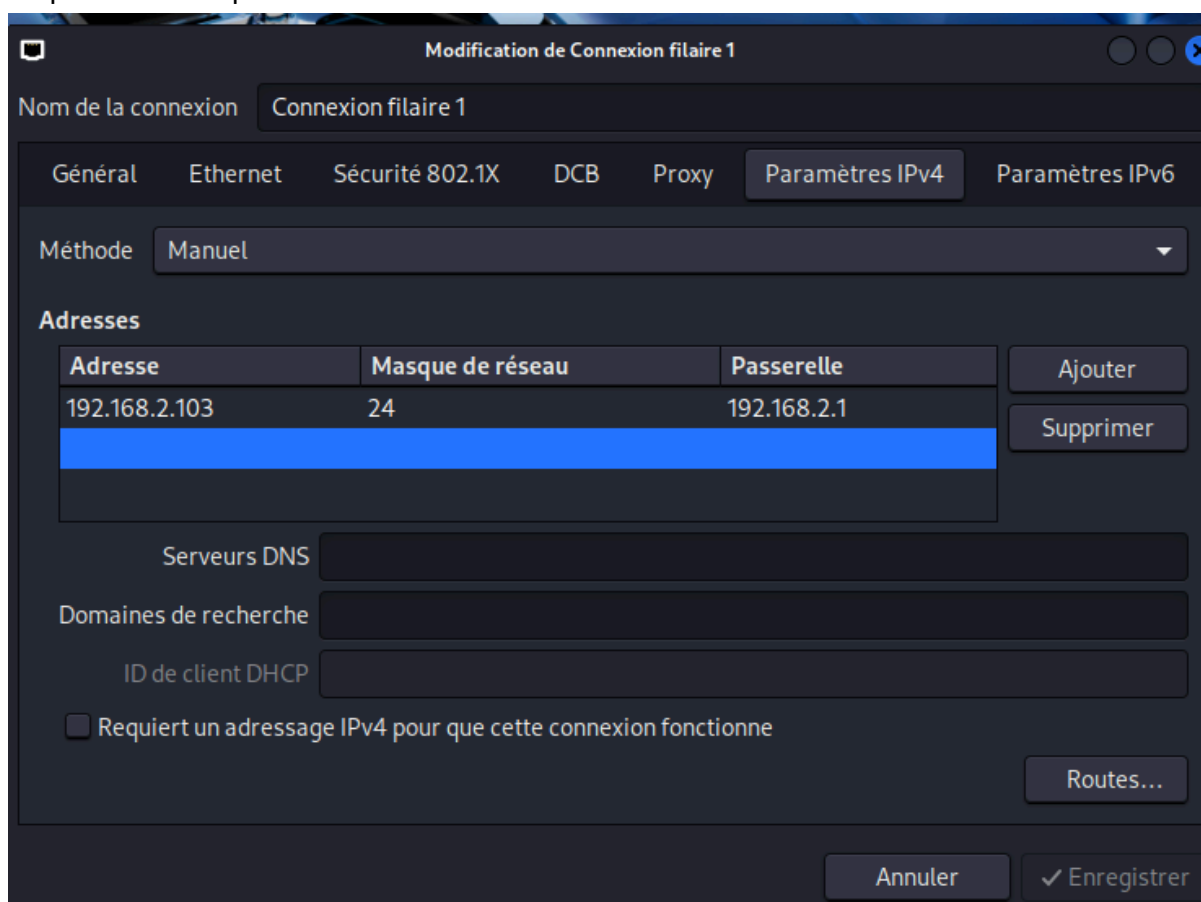
```
(kali@kali)-[~]  
└─$ sudo passwd  
Nouveau mot de passe :  
Retapez le nouveau mot de passe :  
passwd : mot de passe mis à jour avec succès
```



- Configuration des propriétés IPv4 de la carte réseau : cliquer droit sur l'icône Connexion réseau.



Ne pas oublier la passerelle.



- Création d'un réseau NAT appelé NatNetworkSuricata (192.168.2.0/24) et nous modifions le mode d'accès réseau de la VM :



General Options    Redirection de ports

Nom : NatNetworkSuricata

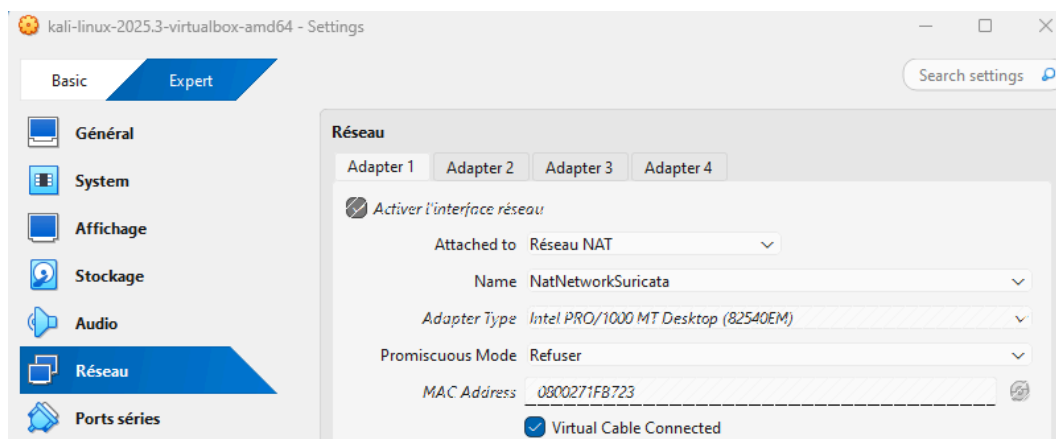
IPv4 Prefix: 192.168.2.0/24

Enable DHCP

Enable IPv6

IPv6 Prefix:

Annoncer la route IPv6 par défaut



- Nous vérifions les paramètres :

```
root@kali: ~  
Session Actions Éditer Vue Aide  
root@kali)~  
# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.2.103/24 brd 192.168.2.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::d929:9df4:9ae0:2ecc/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
root@kali)~  
# ip r  
default via 192.168.2.1 dev eth0 proto static metric 100  
192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.103 metric 100  
root@kali)~  
#
```

## 2) VM Suricata : installer Suricata et jq (json query).

- Configuration de la carte réseau.  
Fait

- Nous modifions les fichiers `/etc/hosts` et `/etc/hostname` puis nous effectuons un reboot pour appliquer les changements

The image shows a terminal window and a network configuration window. The terminal window shows the configuration of `/etc/hostname` and `/etc/hosts`. The network configuration window shows the IPv4 configuration settings.

```
sio@DebSuricata: ~  
GNU nano 8.4 /etc/hostname  
Suricata
```

```
sio@DebSuricata: ~  
GNU nano 8.4 /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 Suricata
```

```
# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

Annuler Filaire Appliquer

Détails Identité IPv4 IPv6 Sécurité

**Méthode IPv4**

Automatique (DHCP)  Réseau local seulement

Manuel  Désactiver

Partagée avec d'autres ordinateurs

**Adresses**

Adresse	Masque de réseau	Passerelle	
192.168.2.101	255.255.255.0	192.168.2.1	⊗
			⊗

**DNS** Automatique

172.17.254.1

Séparer les adresses IP avec des virgules

- Faire un apt-get update et installer suricata :

```
root@Suricata:~# apt-get update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://deb.debian.org/debian trixie-updates InRelease
Réception de : 3 http://security.debian.org/debian-security trixie-security InRelease [43,4 kB]
3,4 ko réceptionnés en 0s (141 ko/s)
Lecture des listes de paquets... Fait
root@Suricata:~#
```

```
root@Suricata:~# apt-get install suricata jq
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
jq est déjà la version la plus récente (1.7.1-6+deb13u1).
jq passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  isa-support libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0 libhttp2
  libhyperscan5 liblua5.1-2 liblua5.1-common libnet1 libnetfilter-log1 libnetfilter-queue1
  librte-bus-pci25 librte-bus-vdev25 librte-eal25 librte-ethdev25 librte-hash25 librte-ip-frag25
  librte-kvargs25 librte-log25 librte-mbuf25 librte-mempool25 librte-meter25 librte-net-bond25
  librte-net25 librte-pci25 librte-rcu25 librte-ring25 librte-sched25 librte-telemetry25 libxdp1
  python3-yaml sse3-support sse4.2-support suricata-update
Paquets suggérés :
  libtcmalloc-minimal4
Paquets recommandés :
  snort-rules-default
Les NOUVEAUX paquets suivants seront installés :
  isa-support libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0 libhttp2
```

Suricata n'est pas démarré :

```
root@Suricata:~# systemctl status suricata
* suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
  Active: failed (Result: exit-code) since Thu 2025-10-16 12:23:59 CEST; 26s ago
  Duration: 132ms
  Invocation: cde88fd21e7346e292d877103e156986
  Docs: man:suricata(8)
       man:suricatasc(8)
       https://suricata.io/documentation/
  Process: 3844 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile
  Main PID: 3845 (code=exited, status=1/FAILURE)

oct. 16 12:23:59 Suricata systemd[1]: suricata.service: Scheduled restart job, restart counter is at 5.
oct. 16 12:23:59 Suricata systemd[1]: suricata.service: Start request repeated too quickly.
oct. 16 12:23:59 Suricata systemd[1]: suricata.service: Failed with result 'exit-code'.
oct. 16 12:23:59 Suricata systemd[1]: Failed to start suricata.service - Suricata IDS/IDP daemon.
lines 1-15/15 (END)
```

### 3) Modification du fichier de configuration /etc/suricata/suricata.yaml :

```
GNU nano 8.4 /etc/suricata/suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.10.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.2.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"

[ 2210 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^J Justifier ^/ Aller ligne M-E Refaire

sio@Suricata: ~
GNU nano 8.4 /etc/suricata/suricata.yaml

# Community Flow ID
# Adds a 'community_id' field to EVE records. These are meant to give
# records a predictable flow ID that can be used to match records to
# output of other tools such as Zeek (Bro).
#
# Takes a 'seed' that needs to be same across sensors and tools
# to make the id less predictable.

# enable/disable the community id feature.
community-id: true
# Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0

# HTTP X-Forwarded-For support by adding an extra field or overwriting
# the source or destination IP address (depending on flow direction)
# with the one reported in the X-Forwarded-For HTTP header. This is
# helpful when reviewing alerts for traffic that is being reverse
# or forward proxied.
xff:

[ 2210 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^J Justifier ^/ Aller ligne M-E Refaire
```

```

GNU nano 8.4 /etc/suricata/suricata.yaml
##
## Step 3: Configure common capture settings
##
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##
# Linux high speed capture support
af-packet:
- interface: enp0s3
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
  # This is only supported for Linux kernel > 3.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket
[ 2210 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^N Remplacer ^U Coller    ^J Justifier ^/ Aller ligneM-E Refaire

```

- Nous devons ajouter à la fin du fichier de configuration pour ne pas avoir à redémarrer le service Suricata après avoir ajouté, supprimé ou modifié des règles :

```

GNU nano 8.4 /etc/suricata/suricata.yaml
##
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config
##
## Include other configs
##
# Includes: Files included here will be handled as if they were in-lined
# in this configuration file. Files with relative pathnames will be
# searched for in the same directory as this configuration file. You may
# use absolute pathnames too.
#include:
# - include1.yaml
# - include2.yaml
detect-engine:
- rule-reload: true
[ 2213 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^N Remplacer ^U Coller    ^J Justifier ^/ Aller ligneM-E Refaire

```

- Vérification du fichier de configuration :

```

sio@Suricata: ~
root@Suricata:~# suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 3
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
root@Suricata:~#

```

- Démarrage de Suricata et nous vérifions son état :

```
root@Suricata:~# systemctl start suricata
root@Suricata:~# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-16 12:30:00 CEST; 7s ago
  Invocation: d9fe87263da9420f9ec0a4eabbcl1a167
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
   Process: 3885 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile >
  Main PID: 3886 (Suricata-Main)
     Tasks: 9 (limit: 4635)
    Memory: 41.8M (peak: 42.4M)
       CPU: 109ms
    CGroup: /system.slice/suricata.service
           └─3886 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/sur>

oct. 16 12:29:59 Suricata systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
oct. 16 12:30:00 Suricata suricata[3885]: i: suricata: This is Suricata version 7.0.10 RELEASE running>
oct. 16 12:30:00 Suricata systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-18/18 (END)
```

- Nous activons le service Suricata pour qu'il soit démarré automatiquement à chaque démarrage de la VM :

```
root@Suricata:~# systemctl enable suricata
-bash: systemctl : commande introuvable
root@Suricata:~# systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-ins
tall.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
root@Suricata:~#
```

## 4) Importer les règles Emerging Threat Open

- Nous consultons l'emplacement et le nom du fichier des règles spécifié dans le fichier de configuration :

```
GNU nano 8.4 /etc/suricata/suricata.yaml
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##
default-rule-path: /var/lib/suricata/rules
rule-files:
- suricata.rules
...
```

- Par défaut, la commande `suricata-update`, saisie sans avoir défini préalablement une autre source, récupère l'ensemble des règles de « Emerging Threats », soit plus de 60 000 règles, dans `/var/lib/suricata/rules/suricata.rules`.

Procédons à l'importation des règles :

```
root@Suricata:~# suricata-update
16/10/2025 -- 12:32:20 - <Info> -- Using data-directory /var/lib/suricata.
16/10/2025 -- 12:32:20 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
16/10/2025 -- 12:32:20 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
16/10/2025 -- 12:32:20 - <Info> -- Found Suricata version 7.0.10 at /usr/bin/suricata.
16/10/2025 -- 12:32:20 - <Info> -- Loading /etc/suricata/suricata.yaml
16/10/2025 -- 12:32:20 - <Info> -- Disabling rules for protocol postgres
16/10/2025 -- 12:32:20 - <Info> -- Disabling rules for protocol modbus
16/10/2025 -- 12:32:20 - <Info> -- Disabling rules for protocol dnp3
16/10/2025 -- 12:32:20 - <Info> -- Disabling rules for protocol enip
16/10/2025 -- 12:32:20 - <Info> -- No sources configured, will use Emerging Threats Open
16/10/2025 -- 12:32:20 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.10/emerging.rules.tar.gz.
100% - 5119959/5119959
16/10/2025 -- 12:32:29 - <Info> -- Done.
16/10/2025 -- 12:32:29 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
2025 -- 12:32:31 - <Info> -- Backing up current rules.
2025 -- 12:32:31 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 61625; enabled: 45822; added: 61625; removed 0; modified: 0
2025 -- 12:32:32 - <Info> -- Writing /var/lib/suricata/rules/classification.config
2025 -- 12:32:32 - <Info> -- Testing with suricata -T.
2025 -- 12:32:51 - <Info> -- Done.
uricata:~#
```

- Nous vérifions la présence du fichier `suricata.rules` :

```
sio@Suricata: ~
root@Suricata:~# cd /var/lib/suricata/rules
root@Suricata:/var/lib/suricata/rules# ls
classification.config suricata.rules
root@Suricata:/var/lib/suricata/rules#
```

- Nous utilisons la commande kill figurant ci-dessous pour prendre en compte les règles importées (ou créées) sans avoir à redémarrer le service Suricata :

```
sio@Suricata: ~
root@Suricata:/var/lib/suricata/rules# cd
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~#
```

- Affichage du contenu du répertoire /var/log/suricata :

```
sio@Suricata: ~
root@Suricata:/var/lib/suricata/rules# cd
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~# ls -l /var/log/suricata
total 580
-rw-r--r-- 1 root root 377246 16 oct. 12:35 eve.json
-rw-r--r-- 1 root root      0 16 oct. 12:23 fast.log
-rw-r--r-- 1 root root 188036 16 oct. 12:35 stats.log
-rw-r--r-- 1 root root 13470 16 oct. 12:35 suricata.log
root@Suricata:~#
```

- Nous affichons le log suricata.log avec la commande tail -f /var/log/suricata/suricata.log et nous redémarrons dans un second terminal le service Suricata :

```
[3886 - Suricata-Main] 2025-10-16 12:35:57 Notice: detect: r
omplete
^C
root@Suricata:~# tail -f /var/log/suricata/suricata.log
```

```
sio@Suricata: ~
sio@Suricata: ~
sio@Suricata:~$ su - root
Mot de passe :
*root@Suricata:~# systemctl restart suricata
```

```
[4327 - Suricata-Main] 2025-10-16 12:38:21 Info: logopenfile: fast output device (regular) initialized: fast.log
[4327 - Suricata-Main] 2025-10-16 12:38:21 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[4327 - Suricata-Main] 2025-10-16 12:38:21 Info: logopenfile: stats output device (regular) initialized: stats.log
[4327 - Suricata-Main] 2025-10-16 12:38:28 Info: detect: 1 rule files processed. 45822 rules successfully loaded, 0 rules failed, 0
[4327 - Suricata-Main] 2025-10-16 12:38:28 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[4327 - Suricata-Main] 2025-10-16 12:38:28 Info: detect: 45825 signatures processed. 963 are IP-only rules, 4414 are inspecting packet payload, 40217 inspect application layer, 109 are decoder event only
[4327 - Suricata-Main] 2025-10-16 12:38:39 Warning: af-packet: enp0s3: AF_PACKET tpacket-v3 is recommended for non-inline operation
[4327 - Suricata-Main] 2025-10-16 12:38:39 Info: runmodes: enp0s3: creating 3 threads
[4327 - Suricata-Main] 2025-10-16 12:38:39 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
[4327 - Suricata-Main] 2025-10-16 12:38:40 Notice: threads: Threads created -> W: 3 FM: 1 FR: 1 Engine started.
```

## 5) Test du bon fonctionnement en mode IDS de Suricata (détection trafic suspect) :

- Installation de curl :

```

sio@Suricata: ~
root@Suricata:~# apt-get install curl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  curl
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 269 kB dans les archives.
Après cette opération, 506 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 curl amd64 8.14.1-2 [269 kB]
269 ko réceptionnés en 0s (759 ko/s)
Sélection du paquet curl précédemment désélectionné.
(Lecture de la base de données... 143535 fichiers et répertoires déjà installés.)
réparation du dépaquetage de ../curl_8.14.1-2_amd64.deb ...
épaquetage de curl (8.14.1-2) ...
aramétrage de curl (8.14.1-2) ...
raitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
oot@Suricata:~#

```

- Test de la règle sid 2100498 (cf. Suricata Quickstart) :

```

GNU nano 8.4 suricata.rules
# alert dns $HOME_NET any -> any any (msg:"ET ADWARE_PUP DNS Query to CoinMiner Proxy Domain (xmrrminingproxy
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ADWARE_PUP Onestart AI Host Profile Checkin (POST)"; f
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ADWARE_PUP Onestart AI Program Version Checkin (POST)";
# alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET ATTACK_RESPONSE Cisco TclShell TFTP Read Request"; con
alert udp $EXTERNAL_NET 69 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Cisco TclShell TFTP Download"; content:"
# alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK_RESPONSE Metasploit/Meterpreter
alert tcp $HOME_NET 139 -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Weak Netbios Lanman Auth Challenge Dete
# alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK_RESPONSE Metasploit/Meterpreter
alert tcp $HOME_NET any -> any any (msg:"ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system"; fl
# alert ip $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ATTACK_RESPONSE id check returned userid"; content:"u
alert udp $HOME_NET 500 -> $EXTERNAL_NET 500 (msg:"GPL ATTACK_RESPONSE isakmp login failed"; content:"|10 05|
# alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ATTACK_RESPONSE directory listing"; flow:established
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; c
alert tcp any any -> any any (msg:"ET ATTACK_RESPONSE Net User Command Response"; flow:established; content:"
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE python shell spawn attempt"; flow:estab
alert tcp $HTTP_SERVERS any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Output of id command from HTTP serv
alert udp $HOME_NET 623 -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Pass
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Microsoft CScript Banner Outbound"; flo
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Microsoft WMIC Prompt Outbound"; flow:e
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Microsoft Netsh Firewall Disable Output
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE SysInternals sc.exe Output Outbound"; f
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (linux sty
root@Suricata:/var/lib/suricata/rules# cd
root@Suricata:~# curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
root@Suricata:~#

```

- Nous vérifions la présence de l'alerte dans le log /var/log/suricata/fast.log :

```

sio@Suricata: ~
root@Suricata:/var/lib/suricata/rules# cd
root@Suricata:~# curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
root@Suricata:~# tail -f /var/log/suricata/fast.log
10/16/2025-12:39:42.589072  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 192.168.2.101-43698 -> 146.75.118.132:80
10/16/2025-12:46:41.715495  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.161.97.21:80 -> 192.168.2.101:35186

```

- Nous vérifions la présence de l'alerte dans le log eve au format json avec la commande jq (permet d'extraire et de lire des données json) :

```

sio@Suricata: ~
root@Suricata:~# jq 'select(.alert | .signature_id==2100498)' /var/log/suricata/eve.json
{
  "timestamp": "2025-10-16T12:46:41.715495+0200",
  "flow_id": 369534165693275,
  "in_iface": "enp0s3",
  "event_type": "alert",
  "src_ip": "18.161.97.21",
  "src_port": 80,
  "dest_ip": "192.168.2.101",
  "dest_port": 35186,
  "proto": "TCP",
  "pkt_src": "wire/pcap",
  "community_id": "1:xLAqTX27A7FTVa7hW6tFvVo/gS8=",
  "tx_id": 0,
  "tx_succeeded": true,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "confidence": [
        "Medium"
      ],
      "created_at": [
        "2010_09_23"
      ],
      "signature_severity": [
        "Informational"
      ],
      "updated_at": [
        "2019_07_26"
      ]
    }
  }
}

```

## 6) Créer 2 règles personnalisées :

- Consulter une règle ICMP du fichier suricata.rules (recherche ctrl + F dans Nano avec itype:8). Etudier de nouveau sa construction. On constate qu'elle est commentée :

```

GNU nano 8.4 suricata.rules
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Echo Reply"; icode:0; itype:0; classtyp>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Fragment Reassembly Time Exceeded"; ico>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IPv6 I-Am-Here undefined code"; icode:>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IPv6 I-Am-Here"; icode:0; itype:34; cla>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IPv6 Where-Are-You undefined code"; ico>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IPv6 Where-Are-You"; icode:0; itype:33;>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IRDP router advertisement"; itype:9; re>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP IRDP router selection"; itype:10; refer>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Information Request undefined code"; ic>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Information Request"; icode:0; itype:15>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP L3retriever Ping"; icode:0; itype:8; co>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Large ICMP Packet"; usize:>800; referen>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Host Redirect undefined code"; i>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Host Redirect"; icode:0; itype:3>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Registration Reply undefined cod>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Registration Reply"; icode:0; it>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Registration Request undefined c>
# alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Mobile Registration Request"; icode:0; i>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP PING *NIX"; itype:8; content:"|10 11 12 1>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP PING BSDtype"; itype:8; content:"|08 09 0>

^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller    ^J Justifier ^/ Aller ligneM-E Refaire

```

- Spécification d'un fichier pour nos propres règles dans le fichier de configuration suricata.yaml :

```

GNU nano 8.4 suricata.yaml
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
- suricata.rules
- custom.rules

##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config

[ 2214 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller    ^J Justifier ^/ Aller ligneM-E Refaire

```

- Nous créons une règle pour déclencher une alerte suite à la réception d'une requête ICMP type 8 :

```

sio@Suricata: ~
GNU nano 8.4 custom.rules
alert icmp $HOME_NET any -> 192.168.2.101 any (msg:"ICMP Echo Request" i:icmp; i:icmp_type:8; sid:1;)

sio@Suricata: ~
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~#

```

- Test de la règle avec les commandes ping, hping3 puis nmap depuis la VM Kali

```

root@kali:~# ping 192.168.2.101
PING 192.168.2.101 (192.168.2.101) 56(84) bytes of data:
64 bytes from 192.168.2.101: icmp_seq=1 ttl=64 time=0.270 ms
64 bytes from 192.168.2.101: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 192.168.2.101: icmp_seq=3 ttl=64 time=0.177 ms
64 bytes from 192.168.2.101: icmp_seq=4 ttl=64 time=0.188 ms
^C
--- 192.168.2.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3860ms
rtt min/avg/max/mdev = 0.177/0.286/0.278/0.437 ms

root@kali:~# hping3 192.168.2.101 --icmp-type 8
HPING 192.168.2.101 (eth0 192.168.2.101): icmp mode set, 28 headers + 0 data
bytes
Vens46 ip=192.168.2.101 ttl=64 id=12243 icmp_seq=0 rtt=3.9 ms
len=46 ip=192.168.2.101 ttl=64 id=12247 icmp_seq=1 rtt=8.1 ms
^C
--- 192.168.2.101 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3.9/6.0/8.1 ms

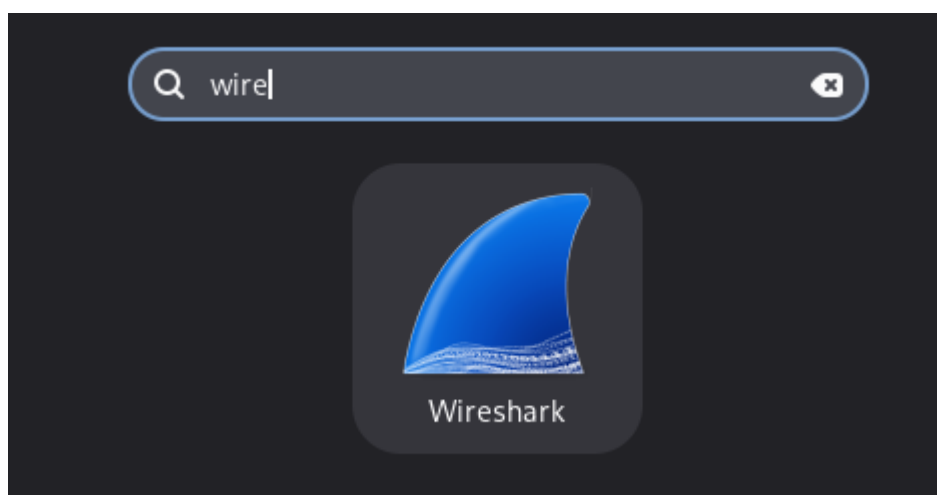
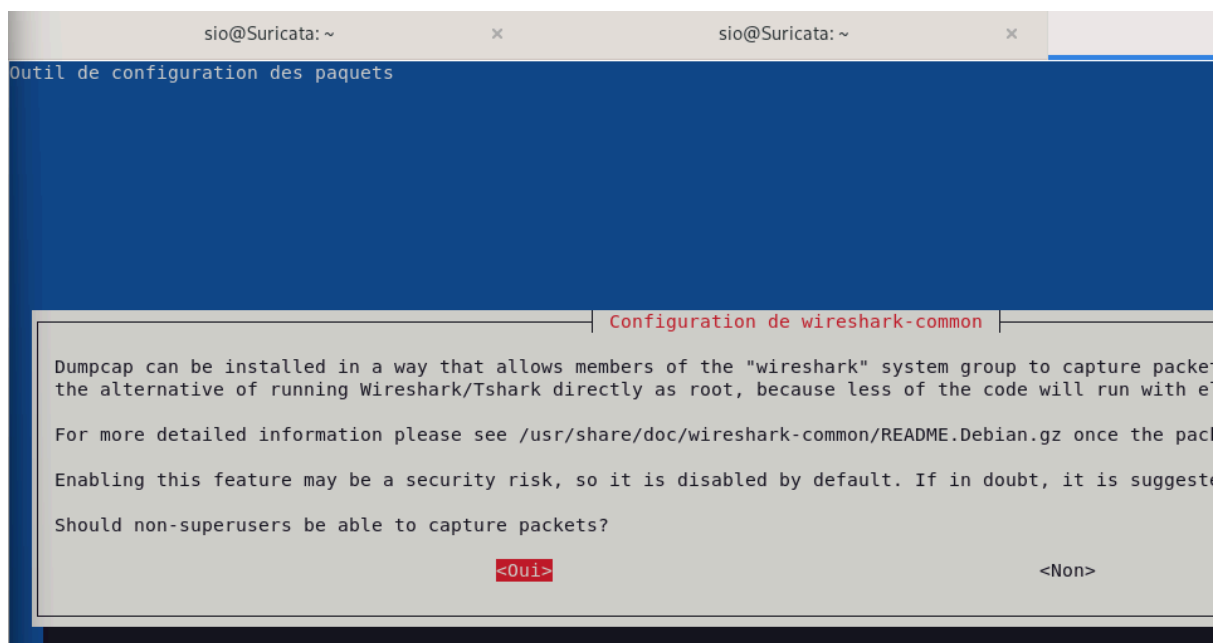
root@kali:~# hping3 192.168.2.101 --icmp-type 3
HPING 192.168.2.101 (eth0 192.168.2.101): icmp mode set, 28 headers + 0 data
bytes
Vens46 ip=192.168.2.101 ttl=64 id=12243 icmp_seq=0 rtt=3.9 ms
len=46 ip=192.168.2.101 ttl=64 id=12247 icmp_seq=1 rtt=8.1 ms
^C
--- 192.168.2.101 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

sio@Suricata:~# tail -f /var/log/suricata/fast.log
10/16/2025-12:39:42.589072 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to
cation: Not Suspicious Traffic [Priority: 3] (TCP) 192.168.2.101:40690 -> 146.75.118.132:80
10/16/2025-12:46:41.715495 [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification:
riority: 2] (TCP) 18.161.97.21:80 -> 192.168.2.101:35186
10/16/2025-15:00:46.127638 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to
cation: Not Suspicious Traffic [Priority: 3] (TCP) 192.168.2.101:51780 -> 146.75.118.132:80
10/16/2025-15:00:46.136777 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to
cation: Not Suspicious Traffic [Priority: 3] (TCP) 192.168.2.101:51780 -> 146.75.118.132:80
10/16/2025-15:00:46.213696 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to
cation: Not Suspicious Traffic [Priority: 3] (TCP) 192.168.2.101:51790 -> 146.75.118.132:80
10/16/2025-15:10:24.362860 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0
10/16/2025-15:10:25.371938 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0
10/16/2025-15:10:26.395821 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0
10/16/2025-15:10:27.422784 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0
10/16/2025-15:11:09.709771 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0
10/16/2025-15:11:10.709669 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] (IC
01:0

```

Nous effectuons un apt-get update et apt-get install wireshark :

```
sio@Suricata:~$ su - root
Mot de passe :
root@Suricata:~# apt-get update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Lecture des listes de paquets... Fait
root@Suricata:~# apt-get install wireshark
```



- Nous lançons une capture avant commande nmap depuis Kali

```

root@kali:~# nmap -sP 192.168.2.101 --disable-arp-ping
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 09:21 EDT
Nmap scan report for 192.168.2.101
Host is up (0.00033s latency).
NMC Address: 00:00:27:1f:0c:8:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
root@kali:~#

```

13	34.811865460	192.168.2.101	192.168.2.103	ICMP	42 Echo (ping)
14	34.811877500	192.168.2.101	192.168.2.103	TCP	54 443 → 38208
15	34.811886370	192.168.2.101	192.168.2.103	TCP	54 80 → 38208
16	34.811894440	192.168.2.101	192.168.2.103	ICMP	54 Timestamp re
17	35.248737044	PCSSystemtec_1f:b7:...	Broadcast	ARP	60 Who has 192
18	37.462332028	192.168.2.101	172.17.254.1	DNS	81 Standard que
19	37.462356078	192.168.2.101	172.17.254.1	DNS	81 Standard que
20	37.463107123	172.17.254.1	192.168.2.101	DNS	136 Standard que
21	37.496891610	172.17.254.1	192.168.2.101	DNS	145 Standard que
22	37.497086187	192.168.2.101	172.233.248.179	NTP	90 NTP Version
23	39.912150151	PCSSystemtec_f0:c8:...	PCSSystemtec_1f:b7:...	ARP	42 Who has 192
24	39.912388901	PCSSystemtec_1f:b7:...	PCSSystemtec_f0:c8:...	ARP	60 192.168.2.10

- Nous créons une seconde règle, destinée à déclencher une alerte suite à un flux SSH, à l'aide des keyword ssh.proto et content.

```

sio@Suricata: ~
GNU nano 8.4 custom.rules
alert icmp $HOME_NET any -> 192.168.2.101 any (msg:"ICMP Echo Request";itype:8;sid:1;)
alert ssh any any -> 192.168.2.101 any (msg:"SSH proto 2";ssh.proto;content:"2.0";sid:2;)
root@Suricata:/var/lib/suricata/rules# cd
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~#

```

- Test d'une connexion ssh depuis Kali au serveur suricata :

The image shows two terminal windows. The top window is a nano editor editing the `/etc/ssh/sshd_config` file on a Suricata server. The configuration includes settings for logging, authentication, and session management. The bottom window shows a Kali machine performing a network scan with Nmap and an SSH connection attempt to the Suricata server. The Nmap output shows the host is up and the SSH service is running. The SSH connection attempt fails due to an authenticity issue. The network traffic capture shows the SSH connection attempt and the resulting traffic.

```

GNU nano 8.4 /etc/ssh/sshd_config
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

[ 124 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich. ^\ Remplacer ^L Coller    ^_ Justifier  ^_/ Aller ligne

root@kali: ~
Session Actions Éditer Vue Aide
root@kali:~# nmap -sP 192.168.2.101 --disable-arp-ping
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 09:27 EDT
Nmap scan report for 192.168.2.101
Host is up (0.00041s latency).
MAC Address: 08:00:27:F0:C8:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

root@kali:~# ssh 192.168.2.101
The authenticity of host '192.168.2.101 (192.168.2.101)' can't be established.
ED25519 key fingerprint is SHA256:U2HBkaYk/uk7oE4AuYwe2Izjv0FykLN4bNcAtnWLT6w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?

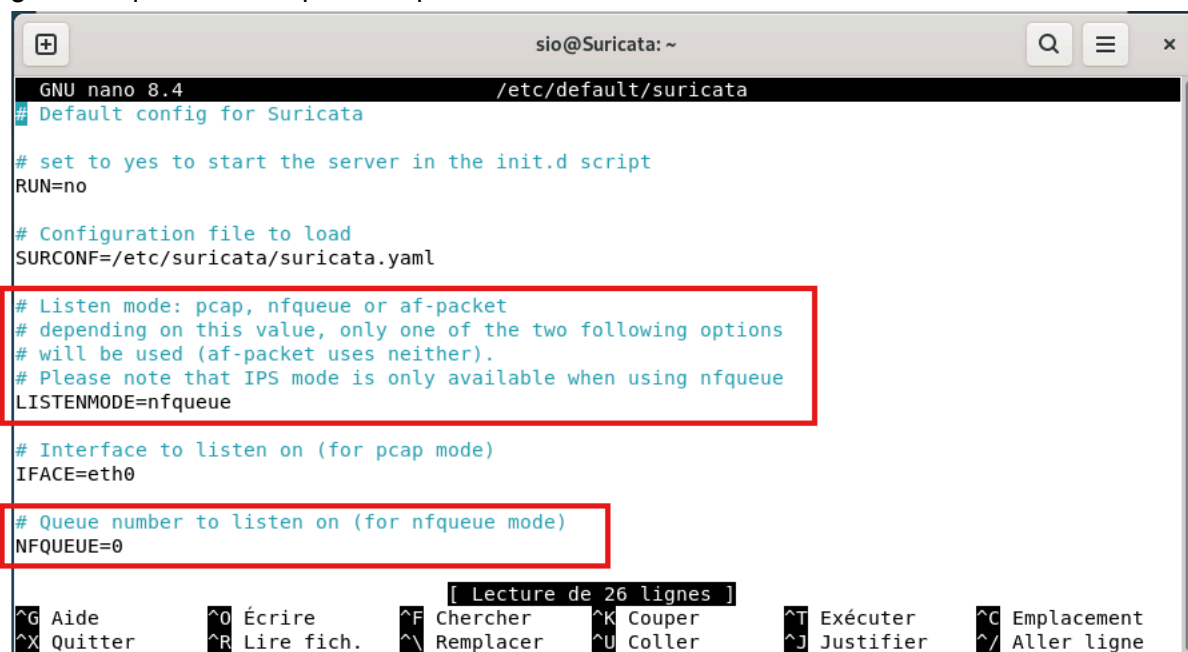
sio@Suricata: ~
related to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:14:01.357169 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely r
elated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:14:02.120631 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely r
elated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:14:02.375053 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely r
elated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:14:02.513158 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely r
elated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:14:03.442713 [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely r
elated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 19
2.168.2.101:36464 -> 146.75.118.132:80
10/16/2025-15:21:15.176522 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priorit
y: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-15:27:19.863942 [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priorit
y: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-15:36:42.451350 [**] [1:2:0] SSH proto 2 [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.2.103:47324 -> 192.168.2.101:22

```

## 7) Basculer Suricata en mode IPS :

### a) Configuration de Suricata :

- Nous vérifions dans le fichier `/etc/default/suricata` que la directive `LISTENMODE` soit déjà égale à `nfqueue` et non pas à `af-packet` :



```
GNU nano 8.4 /etc/default/suricata
# Default config for Suricata

# set to yes to start the server in the init.d script
RUN=no

# Configuration file to load
SURCONF=/etc/suricata/suricata.yaml

# Listen mode: pcap, nfqueue or af-packet
# depending on this value, only one of the two following options
# will be used (af-packet uses neither).
# Please note that IPS mode is only available when using nfqueue
LISTENMODE=nfqueue

# Interface to listen on (for pcap mode)
IFACE=eth0

# Queue number to listen on (for nfqueue mode)
NFQUEUE=0
```

- Pour activer le mode `nfqueue` manuellement (à saisir à nouveau au prochain redémarrage du serveur) :

```
root@Suricata:~# suricata -c /etc/suricata/suricata.yaml -q 0
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
i: threads: Threads created -> RX: 1 W: 3 TX: 1 FM: 1 FR: 1 Engine started.
^Ci: suricata: Signal Received. Stopping engine.
i: nfq: (RX-NFQ#0) Treated: Pkts 0, Bytes 0, Errors 0
i: nfq: (RX-NFQ#0) Verdict: Accepted 0, Dropped 0, Replaced 0
root@Suricata:~#
```

- Pour activer automatiquement le mode nfqueue à chaque démarrage du service suricata :  
Systemctl edit suricata

```

GNU nano 8.4 /etc/systemd/system/suricata.service.d/.#override.confbfda2e5f6b174017
# Description=Suricata IDS/IDP daemon
# After=network.target network-online.target
# Requires=network-online.target
# Documentation=man:suricata(8) man:suricatasc(8)
# Documentation=https://suricata.io/documentation/
#
[Service]
ExecStart=
ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid -q 0 -vvv
Type=simple

```

[ 20 lignes écrites ]

<sup>^</sup>G Aide    <sup>^</sup>O Écrire    <sup>^</sup>F Chercher    <sup>^</sup>K Couper    <sup>^</sup>T Exécuter    <sup>^</sup>C Emplacement    <sup>M-U</sup> Annuler  
<sup>^</sup>X Quitter    <sup>^</sup>R Lire fich.    <sup>^</sup>N Remplacer    <sup>^</sup>U Coller    <sup>^</sup>J Justifier    <sup>^</sup>/ Aller ligne    <sup>M-E</sup> Refaire

- Nous rechargeons systemd puis nous redémarrons suricata et pour ainsi vérifier son état :

```

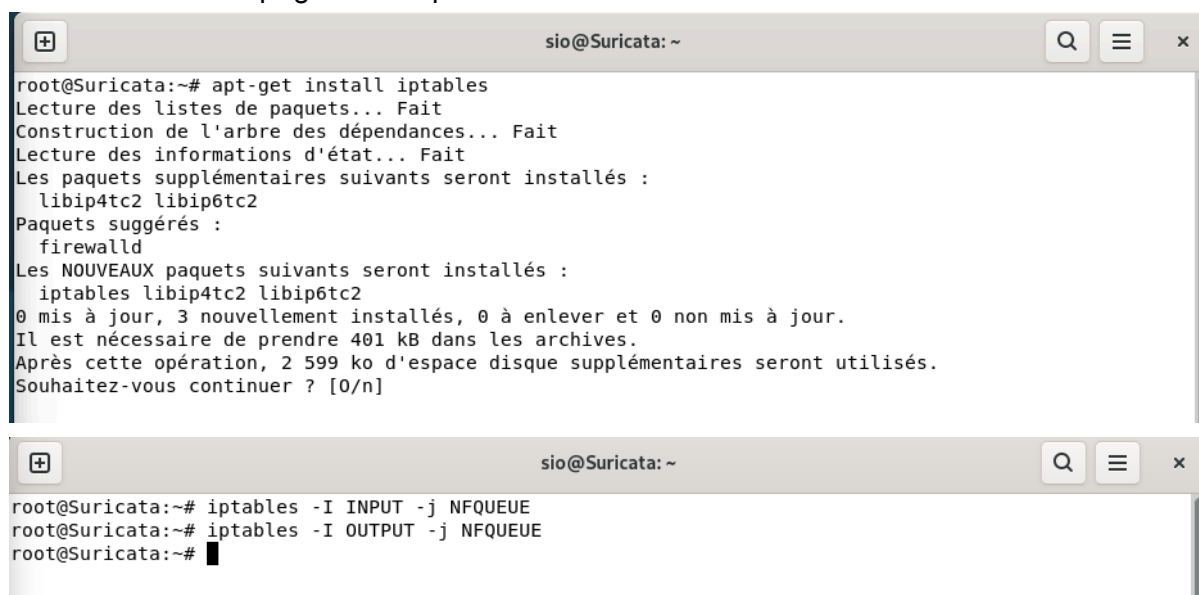
root@Suricata:~# systemctl daemon-reload
root@Suricata:~# systemctl restart suricata
root@Suricata:~# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-16 15:54:25 CEST; 7s ago
 Invocation: de0d0161a7b14757b7c2745f4932a34b
   Docs: man:suricata(8)
         man:suricatasc(8)
         https://suricata.io/documentation/
 Main PID: 2983 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile>
   Tasks: 1 (limit: 4635)
  Memory: 300.3M (peak: 300.3M)
     CPU: 7.591s
   CGroup: /system.slice/suricata.service
           └─2985 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/su>

oct. 16 15:54:25 Suricata systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
oct. 16 15:54:25 Suricata suricata[2983]: i: suricata: This is Suricata version 7.0.10 RELEASE runnin>
oct. 16 15:54:25 Suricata systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-18/18 (END)

```

## b) Configurer IPTables (NFQUEUE)

- Nous effectuons apt-get install iptables



The image shows two terminal windows from a Linux system. The first window shows the command 'apt-get install iptables' being executed. The output indicates that the installation is successful, listing additional packages like 'libip4tc2' and 'libip6tc2' that will be installed along with 'iptables'. It also shows the disk space requirements. The second window shows the configuration of iptables for the INPUT and OUTPUT chains using the 'NFQUEUE' target.

```
sio@Suricata: ~  
root@Suricata:~# apt-get install iptables  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  libip4tc2 libip6tc2  
Paquets suggérés :  
  firewallld  
Les NOUVEAUX paquets suivants seront installés :  
  iptables libip4tc2 libip6tc2  
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.  
Il est nécessaire de prendre 401 kB dans les archives.  
Après cette opération, 2 599 ko d'espace disque supplémentaires seront utilisés.  
Souhaitez-vous continuer ? [0/n]  
  
sio@Suricata: ~  
root@Suricata:~# iptables -I INPUT -j NFQUEUE  
root@Suricata:~# iptables -I OUTPUT -j NFQUEUE  
root@Suricata:~# █
```

## 8) Test du bon fonctionnement du mode IPS :

- Nous modifions l'action de la règle concernant les trames ICMP Echo Request :

```

sio@Suricata: ~
GNU nano 8.4 /var/lib/suricata/rules/custom.rules
drop icmp $HOME_NET any -> 192.168.2.101 any (msg:"ICMP Echo Request";itype:8;sid:1;)
alert ssh any any -> 192.168.2.101 any (msg:"SSH proto 2";ssh.proto;content:"2.0";sid:2;)

[ 2 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher ^K Couper   ^T Exécuter ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller   ^J Justifier ^_ Aller ligne M-E Refaire

root@Suricata:~# iptables -I INPUT -j NFQUEUE
root@Suricata:~# iptables -I OUTPUT -j NFQUEUE
root@Suricata:~# nano /var/lib/suricata/rules/custom.rules
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~#

```

- Nous effectuons un ping depuis Kali et nous vérifions dans le log fast.log que l'action Drop a bien été effectuée par Suricata :

```

root@kali:~# ping 192.168.2.101
PING 192.168.2.101 (192.168.2.101) 56(84) bytes of data:
^C
--- 192.168.2.101 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2047ms

32.255332 [wDrop]** [1:1:0] ICMP Echo Request** [Classification: (null)] [Prio
192.168.2.103:8 -> 192.168.2.101:0
33.280377 [wDrop]** [1:1:0] ICMP Echo Request** [Classification: (null)] [Prio
192.168.2.103:8 -> 192.168.2.101:0

```

- Modification dans le fichier `suricata.rules` l'action de la règle dont le sid est 2100498 (cf. test page 21) :

```

sio@Suricata: ~
GNU nano 8.4 /var/lib/suricata/rules/suricata.rules
# alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET ATTACK RESPONSE Cisco TclShell TFTP Read Request"; content:"|00 01 74 63 6C 73 6
alert udp $EXTERNAL_NET 69 -> $HOME_NET any (msg:"ET ATTACK RESPONSE Cisco TclShell TFTP Download"; content:"|54 63 6C 53 68 65 6C 6C|
# alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Co
alert tcp $HOME_NET 139 -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Weak Netbios Lanman Auth Challenge Detected"; flow:from_server; c
# alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Co
alert tcp $HOME_NET any -> any any (msg:"ET ATTACK RESPONSE Possible MS CMD Shell opened on local system"; flow:established; dsize:<110
# alert ip $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ATTACK RESPONSE id check returned userid"; content:"uid="; byte_test:5,<,65537,
alert udp $HOME_NET 500 -> $EXTERNAL_NET 500 (msg:"GPL ATTACK RESPONSE isakmp Login failed"; content:"|10 05|"; depth:2; offset:17; con
# alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ATTACK RESPONSE directory listing"; flow:established; content:"Volume Serial N
drop ip any any -> any any (msg:"GPL ATTACK RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2
alert tcp any any -> any any (msg:"ET ATTACK RESPONSE Net User Command Response"; flow:established; content:"User accounts for |5C 5C|
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK RESPONSE python shell spawn attempt"; flow:established,to_client; content:
alert tcp $HTTP_SERVERS any -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Output of id command from HTTP server"; flow:established; con
alert udp $HOME_NET 623 -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP m
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Microsoft CScript Banner Outbound"; flow:established; content:"Wi
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Microsoft WMI Prompt Outbound"; flow:established; content:"wmic|
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE Microsoft Netsh Firewall Disable Output Outbound"; flow:establish
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK RESPONSE SysInternals sc.exe Output Outbound"; flow:established; content:"
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET ATTACK RESPONSE Possible /etc/passwd via SMTP (linux style)"; flow:established,to
[ 61625 lignes écrites ]
^G Aide          ^O Écrire        ^F Chercher      ^K Couper        ^T Exécuter     ^C Emplacement  M-U Annuler     M-A Marquer
^X Quitter      ^R Lire fich.   ^N Remplacer    ^U Coller       ^J Justifier    ^/ Aller ligne  M-E Refaire     M-6 Copier

```

```

sio@Suricata: ~
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~#

```

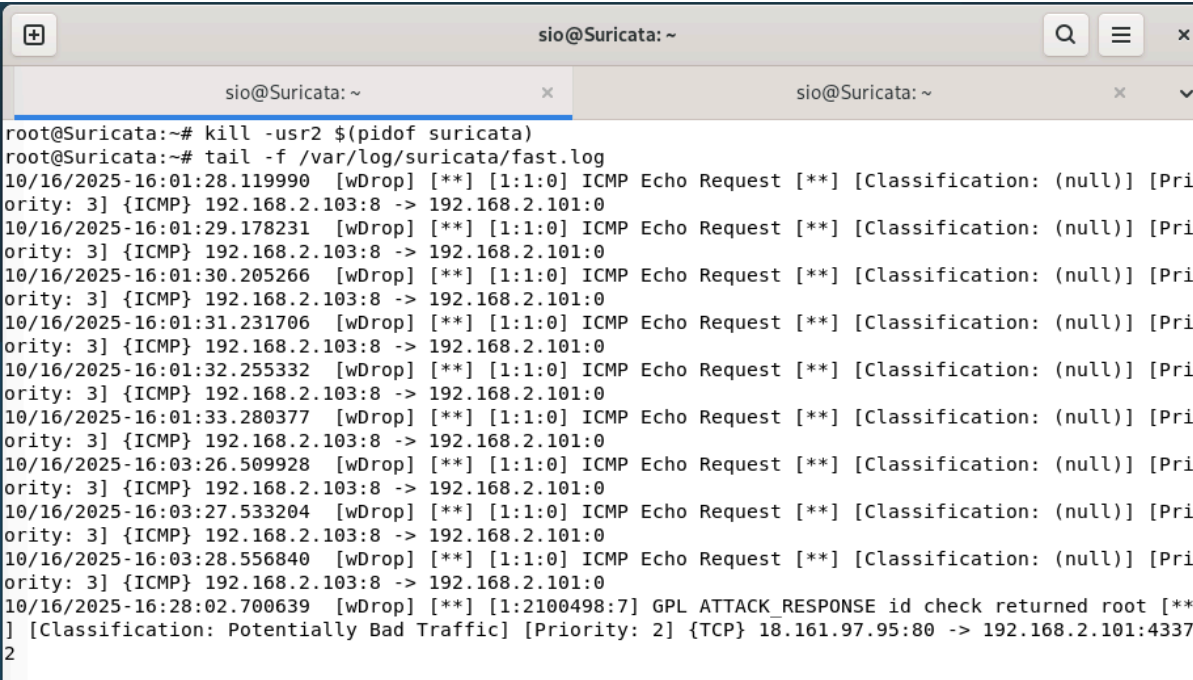
- Test avec la commande `curl` :

```

sio@Suricata: ~
sio@Suricata:~$ su -
Mot de passe :
root@Suricata:~# curl --max-time 5 http://testmynids.org/uid/index.html
curl: (28) Resolving timed out after 5000 milliseconds
root@Suricata:~#

```

- Vérification de l'action Drop dans le log fast.log :



```
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~# tail -f /var/log/suricata/fast.log
10/16/2025-16:01:28.119990 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:01:29.178231 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:01:30.205266 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:01:31.231706 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:01:32.255332 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:01:33.280377 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:03:26.509928 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:03:27.533204 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:03:28.556840 [wDrop] [**] [1:1:0] ICMP Echo Request [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.2.103:8 -> 192.168.2.101:0
10/16/2025-16:28:02.700639 [wDrop] [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.161.97.95:80 -> 192.168.2.101:43372
```

## 9) Créer une règle permettant de bloquer une attaque DOS (SYN Flood) sans bloquer les requêtes http légitimes :

```

sio@Suricata: ~
GNU nano 8.4 /var/lib/suricata/rules/custom.rules
drop icmp $HOME_NET any -> 192.168.2.101 any (msg:"ICMP Echo Request";itype:8;sid:1;)
alert ssh any any -> 192.168.2.101 any (msg:"SSH proto 2";ssh.proto;content:"2.0";sid:2;)
alert tcp any any -> 192.168.2.101 80 (msg:"HPING3 DOS";ttl:64;flow:to_server;flags:S;classtype:attempted-dos;sid:3;rev:1;)

```

```

sio@Suricata: ~
GNU nano 8.4 /etc/suricata/threshold.config
# Thresholding:
#
# This feature is used to reduce the number of logged alerts for noisy rules.
# Thresholding commands limit the number of times a particular event is logged
# during a specified time interval.

rate_filter gen_id 1, sig_id 3, track by_dst, count 100, seconds 5, new_action drop, timeout 30

# The syntax is the following:
#
# threshold gen_id <gen_id>, sig_id <sig_id>, type <limit|threshold|both>, track <by_src|by_dst>, coun
#
# event_filter gen_id <gen_id>, sig_id <sig_id>, type <limit|threshold|both>, track <by_src|by_dst>, c
#
# suppress gen_id <gid>, sig_id <sid>
# suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst>, ip <ip|subnet>
#
# The options are documented at https://docs.suricata.io/en/latest/configuration/global-thresholds.htm
#
# Please note that thresholding can also be set inside a signature. The interaction between rule based
[ 34 lignes écrites ]
^G Aide      ^O Écrire    ^F Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich.^N Remplacer ^U Coller    ^J Justifier ^/ Aller ligne M-E Refaire

```

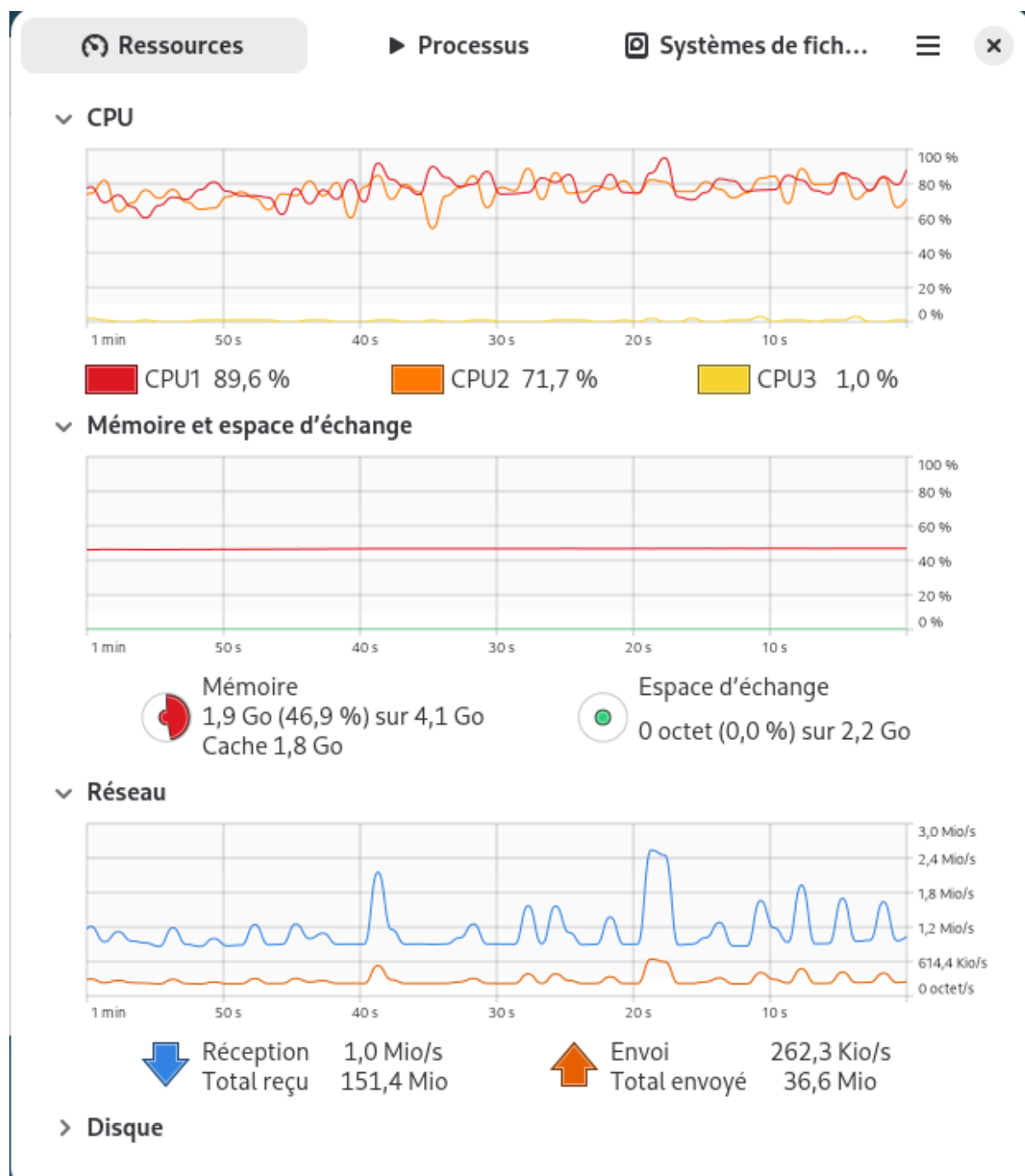
```

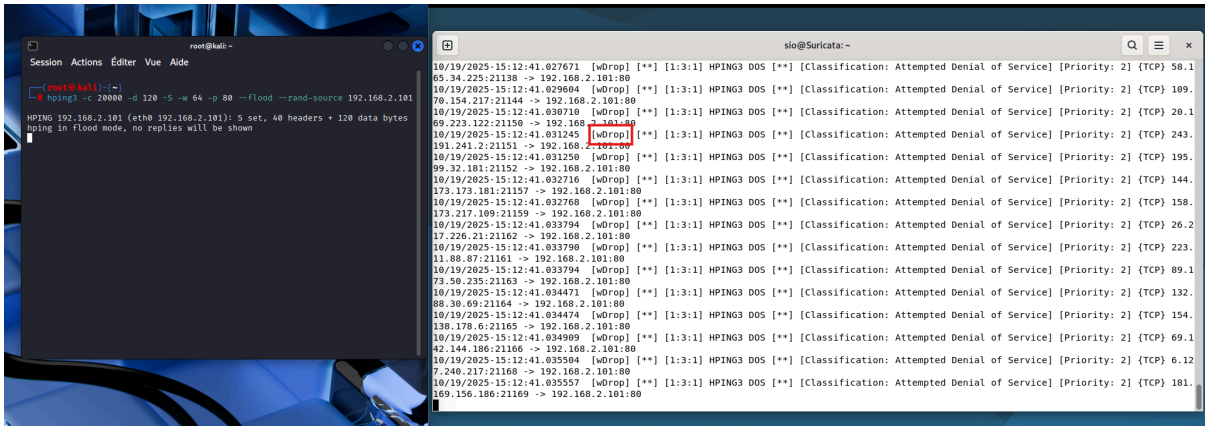
sio@Suricata: ~
root@Suricata:~# kill -usr2 $(pidof suricata)
root@Suricata:~# █

```

- Nous démarrons une capture de trames sur la machine Suricata puis démarrons l'attaque DOS SYN Flood avec hping3 et nous vérifions la suppression des paquets ainsi que la disponibilité de la machine Suricata :

Nous vérifions également avec l'application Moniteur système l'utilisation des ressources CPU/RAM de la machine Suricata.





Capture en cours de enp0s3

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3712...	3.212255331	192.168.2.101	16.52.105.148	TCP	58 80	→ 500
3712...	3.212260951	192.168.2.101	73.41.159.17	TCP	58 80	→ 501
3712...	3.212288751	21.171.134.188	192.168.2.101	TCP	174 502	→ 80
3712...	3.212288821	86.250.174.59	192.168.2.101	TCP	174 503	→ 80
3712...	3.212288871	148.22.71.211	192.168.2.101	TCP	174 504	→ 80
3712...	3.212288911	123.150.123.169	192.168.2.101	TCP	174 505	→ 80
3712...	3.212288951	91.58.58.64	192.168.2.101	TCP	60 498	→ 80
3712...	3.212288991	55.54.193.152	192.168.2.101	TCP	60 499	→ 80
3712...	3.212289031	16.52.105.148	192.168.2.101	TCP	60 500	→ 80
3712...	3.212296441	192.168.2.101	21.171.134.188	TCP	58 80	→ 502
3712...	3.212303471	192.168.2.101	86.250.174.59	TCP	58 80	→ 503
3712...	3.212309011	192.168.2.101	148.22.71.211	TCP	58 80	→ 504
3712...	3.212314651	192.168.2.101	123.150.123.169	TCP	58 80	→ 505
3712...	3.212342621	73.41.159.17	192.168.2.101	TCP	60 501	→ 80
3712...	3.212342681	17.164.105.233	192.168.2.101	TCP	174 506	→ 80
3712...	3.212342721	113.168.64.118	192.168.2.101	TCP	174 507	→ 80
3712...	3.212342761	144.39.218.106	192.168.2.101	TCP	174 508	→ 80
3712...	3.212342801	21.171.134.188	192.168.2.101	TCP	60 502	→ 80
3712...	3.212342841	86.250.174.59	192.168.2.101	TCP	60 503	→ 80
3712...	3.212342881	148.22.71.211	192.168.2.101	TCP	60 504	→ 80
3712...	3.212342921	123.150.123.169	192.168.2.101	TCP	60 505	→ 80
3712...	3.212351561	192.168.2.101	17.164.105.233	TCP	58 80	→ 506

Frame 1: 80 bytes on wire (720 bits)