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

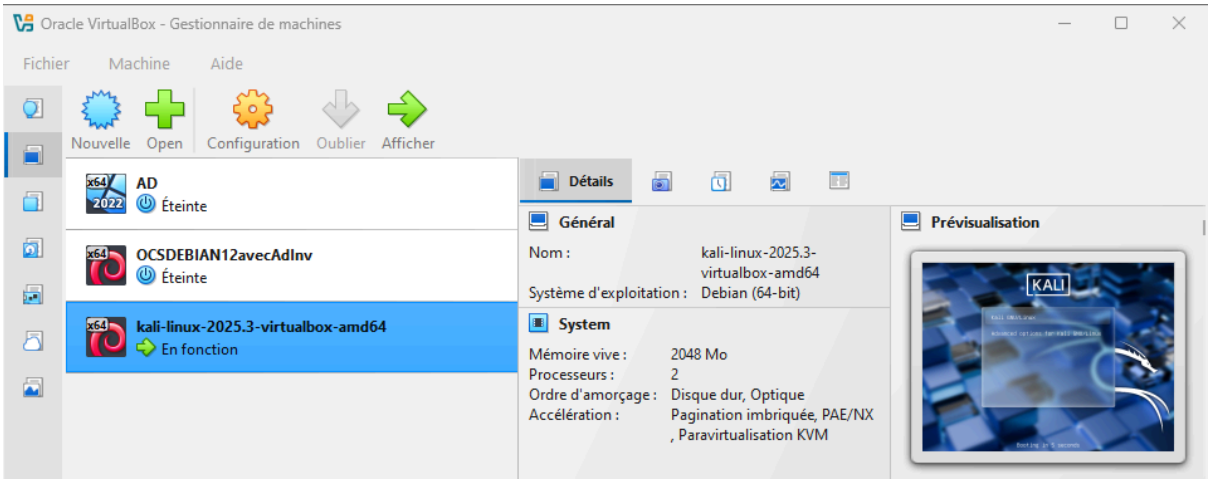
## Table des matières :

# 1. Travail à faire.

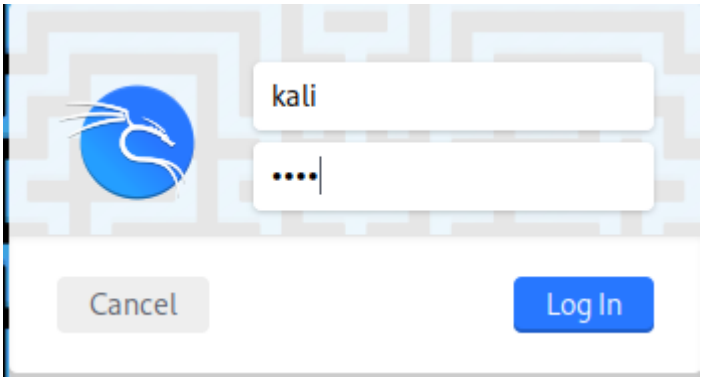
1. Configurer Kali 2025 ;
2. Installation de Suricata, du serveur SSH et du serveur Web sur la VM Suricata ;
3. Configurer Suricata ;
4. Importer l'ensemble des règles ET Open (fichier suricata.rules) ;
5. Tester le bon fonctionnement de Suricata en tant que HIDS (cf. commande curl et la règle sid
2100498 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 :

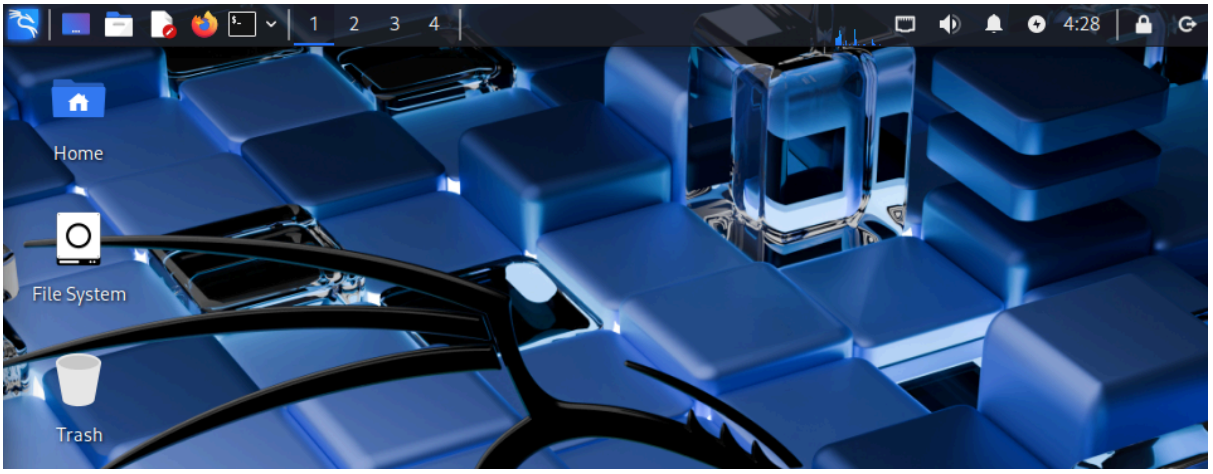
La VM kalilinux a été récupérée




Utilisateur : kali ; Mot de passe : kali
Nous saisissons kqli sur le clavier que ce soit pour l'utilisateur et le mot de passe

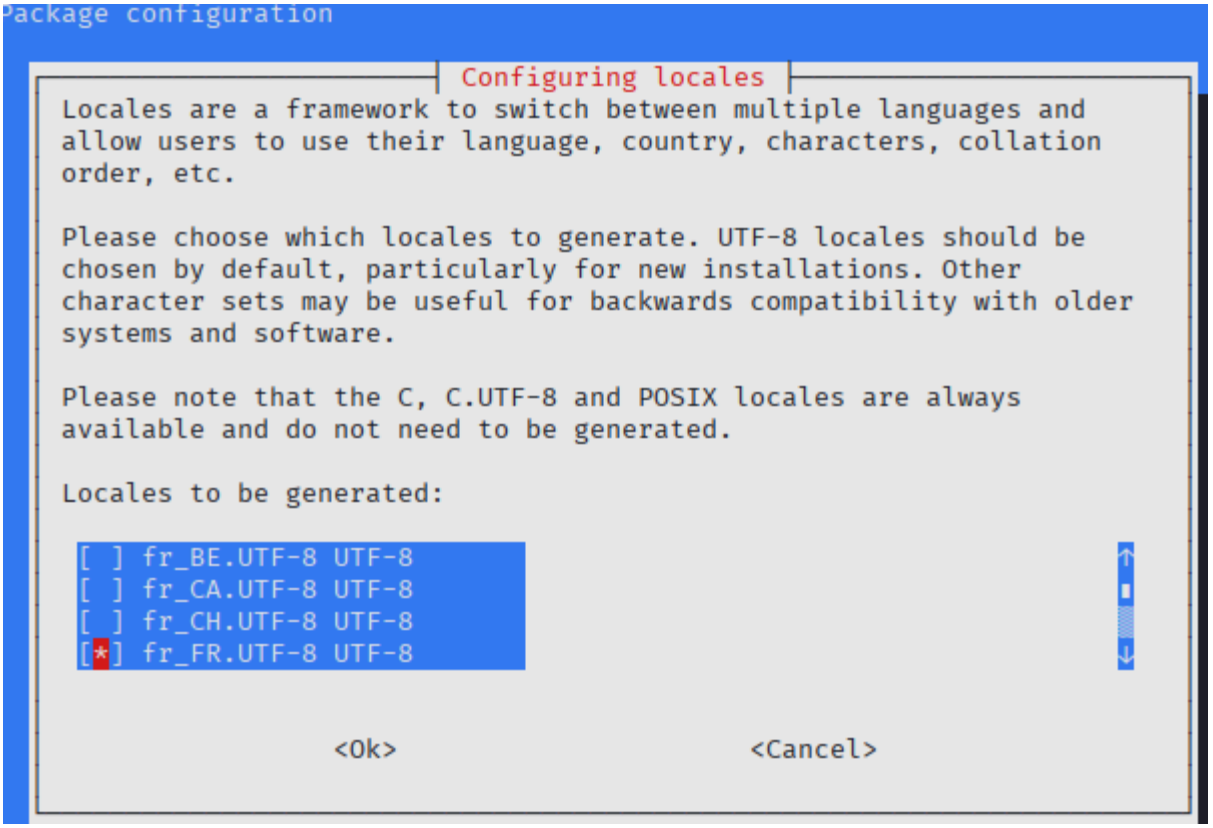


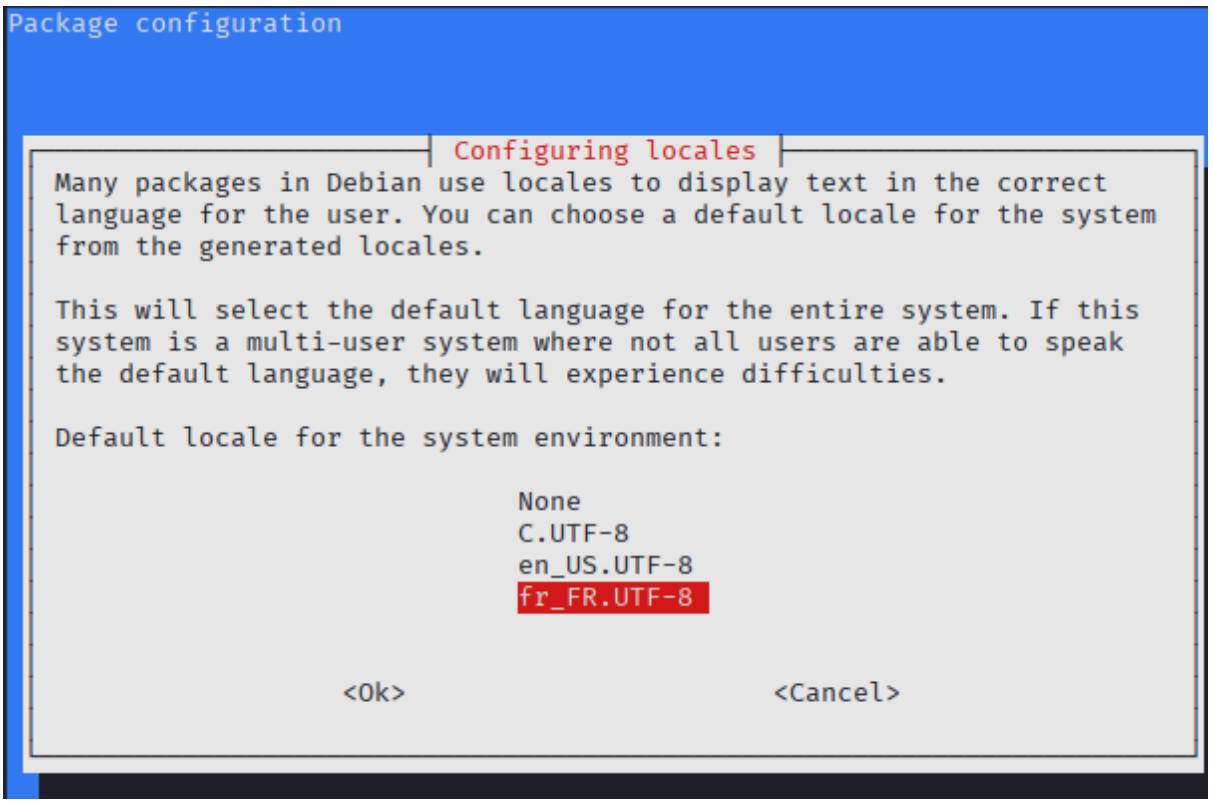

Les additions invités sont déjà ajoutées à la VM.



▪ Nous allons mettre l'interface graphique en Français :

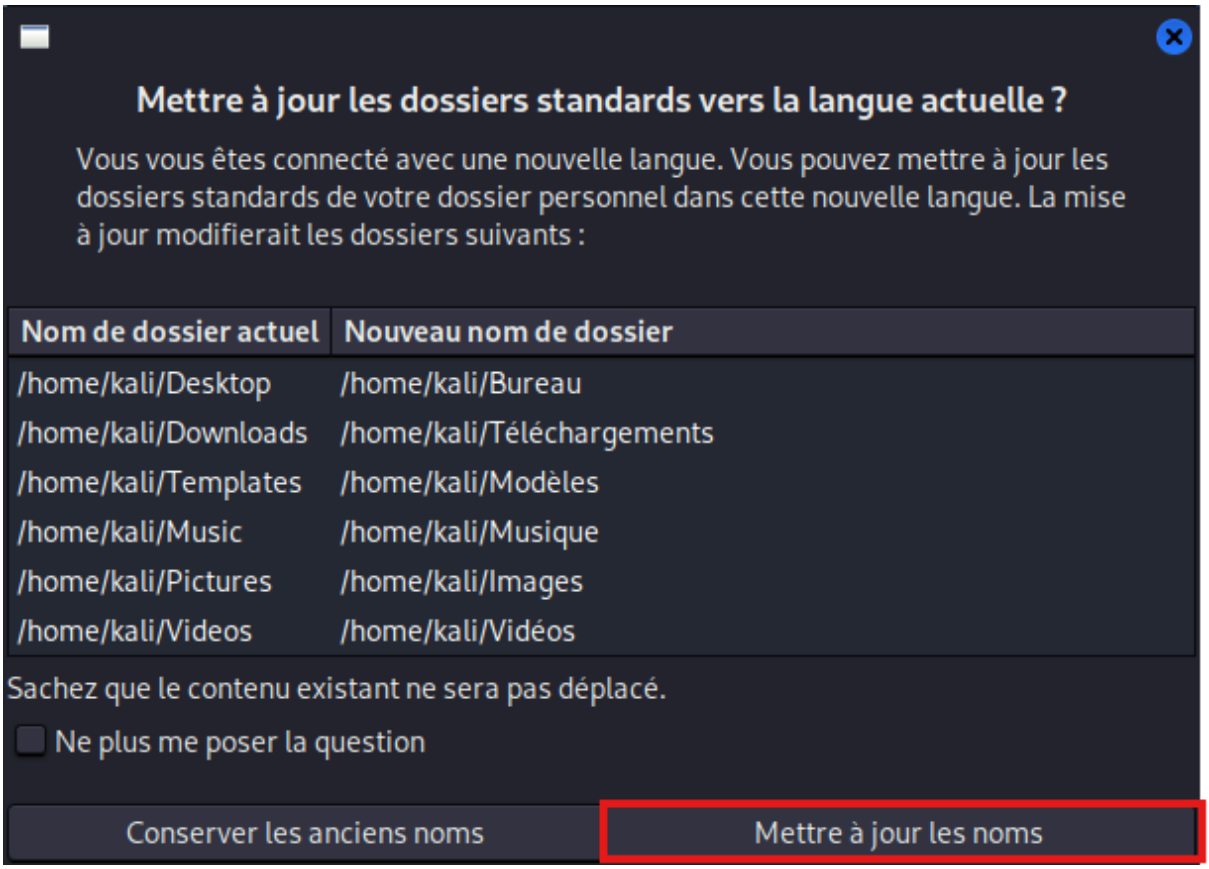
```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg-reconfigure locales
[sudo] password for kali:
```



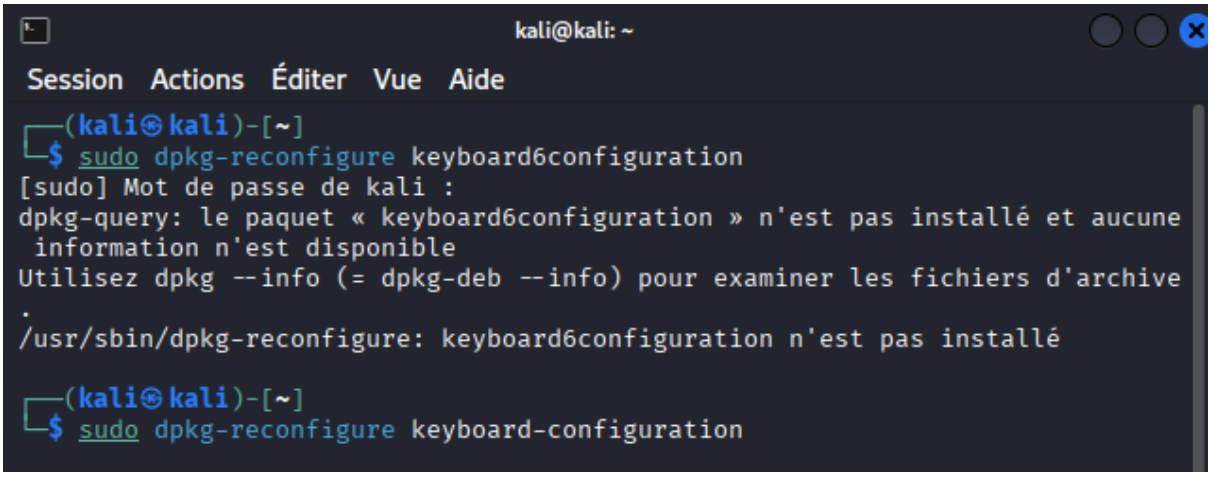


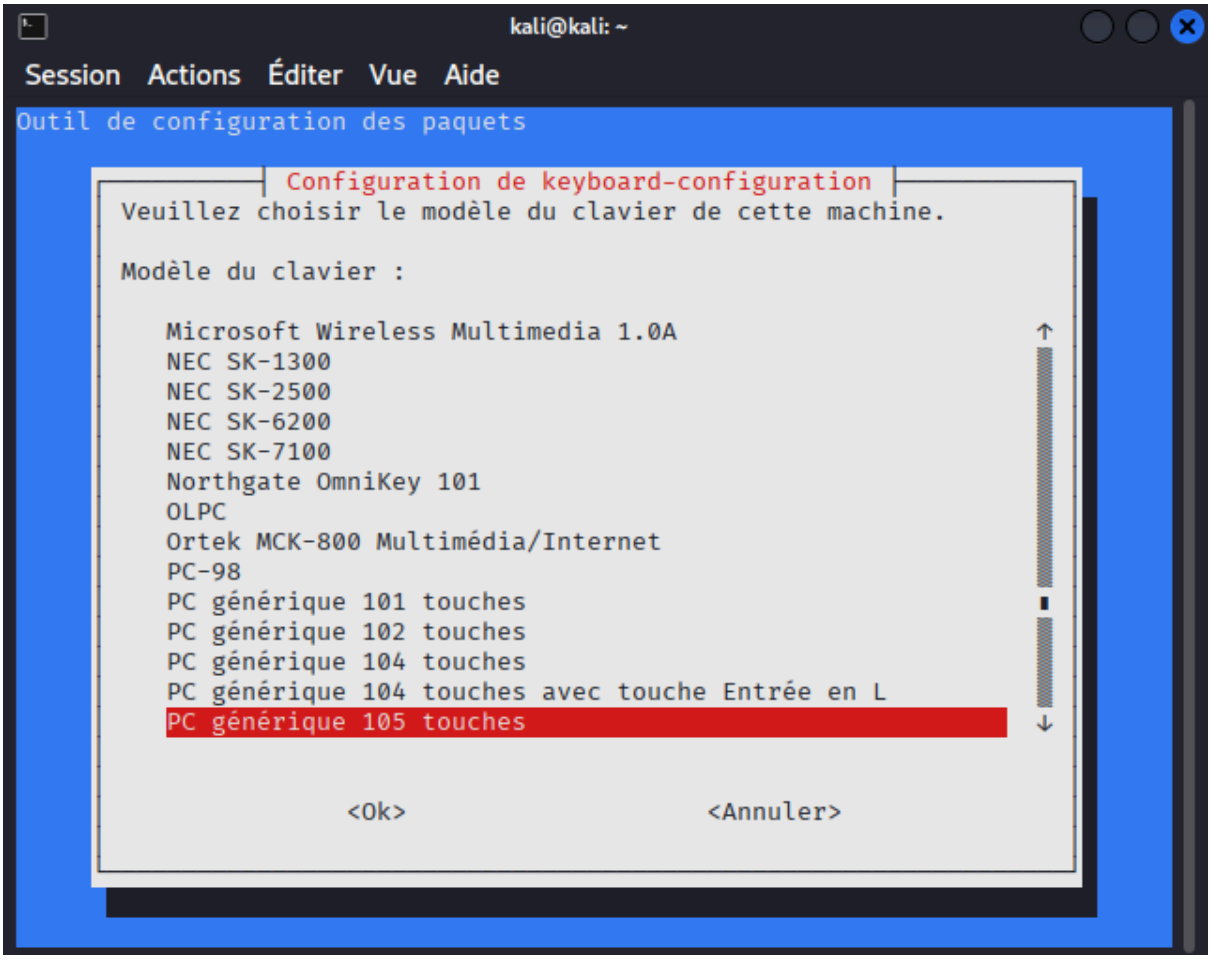

```
┌──(kali㉿kali)-[~]
└─$ sudo dpkg-reconfigure locales
Generating locales (this might take a while)...
  en_US.UTF-8... done
  fr_FR.UTF-8... done
Generation complete.
```

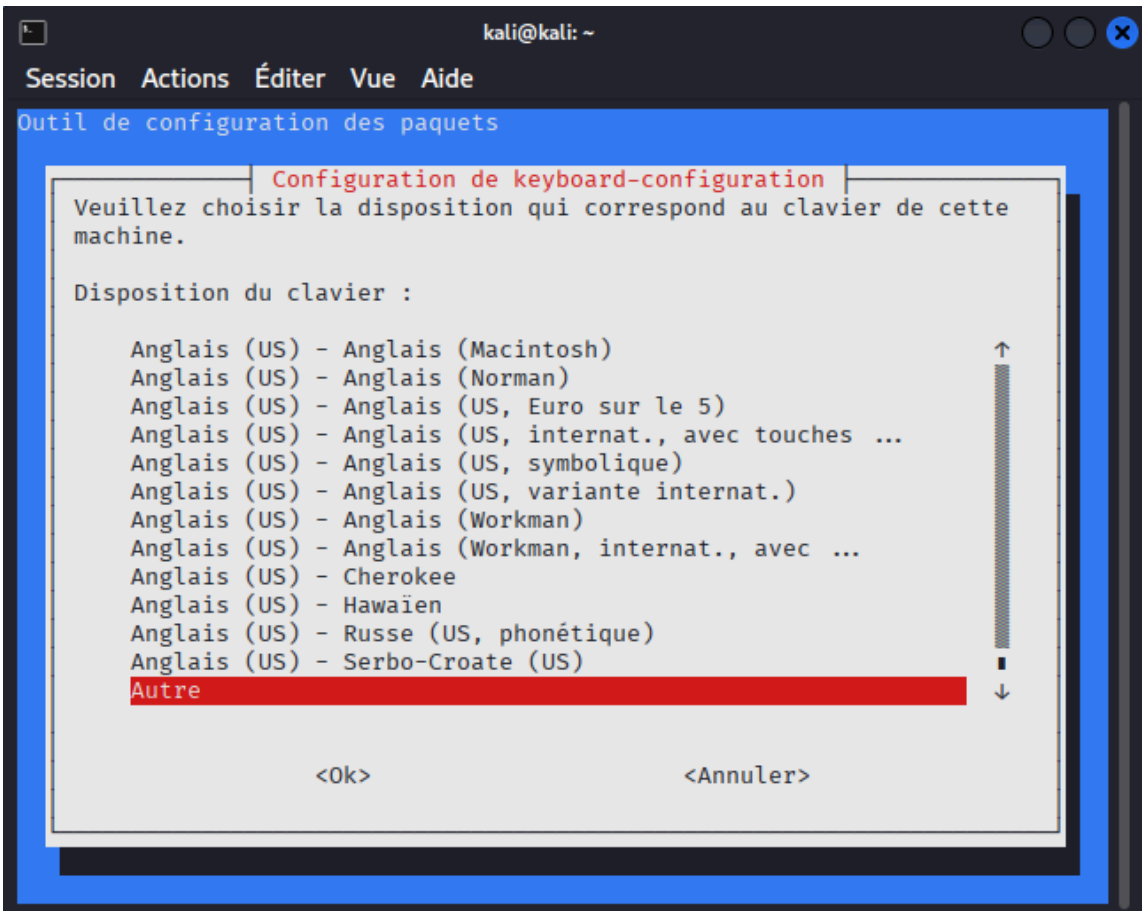
Au redémarrage, nous devons saisir de nouveau kqli comme le clavier est encore en qwerty.

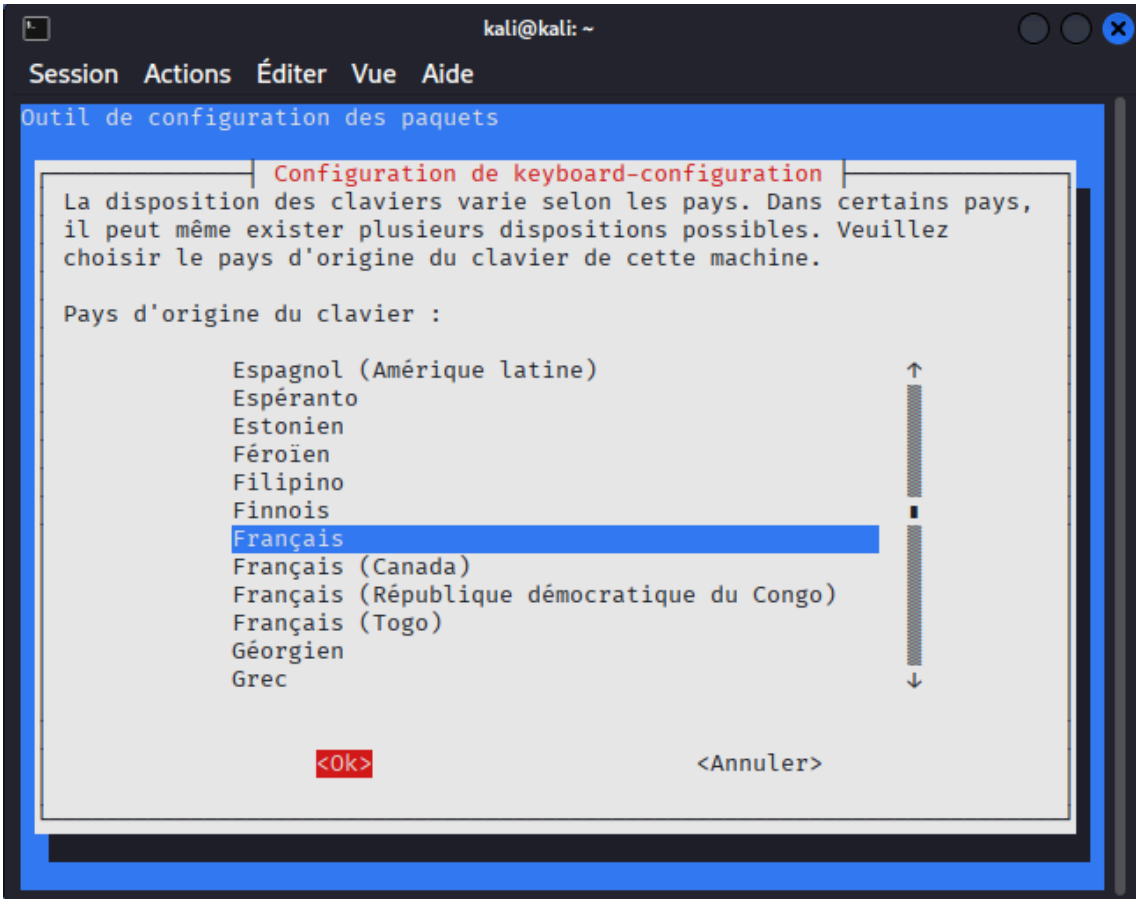


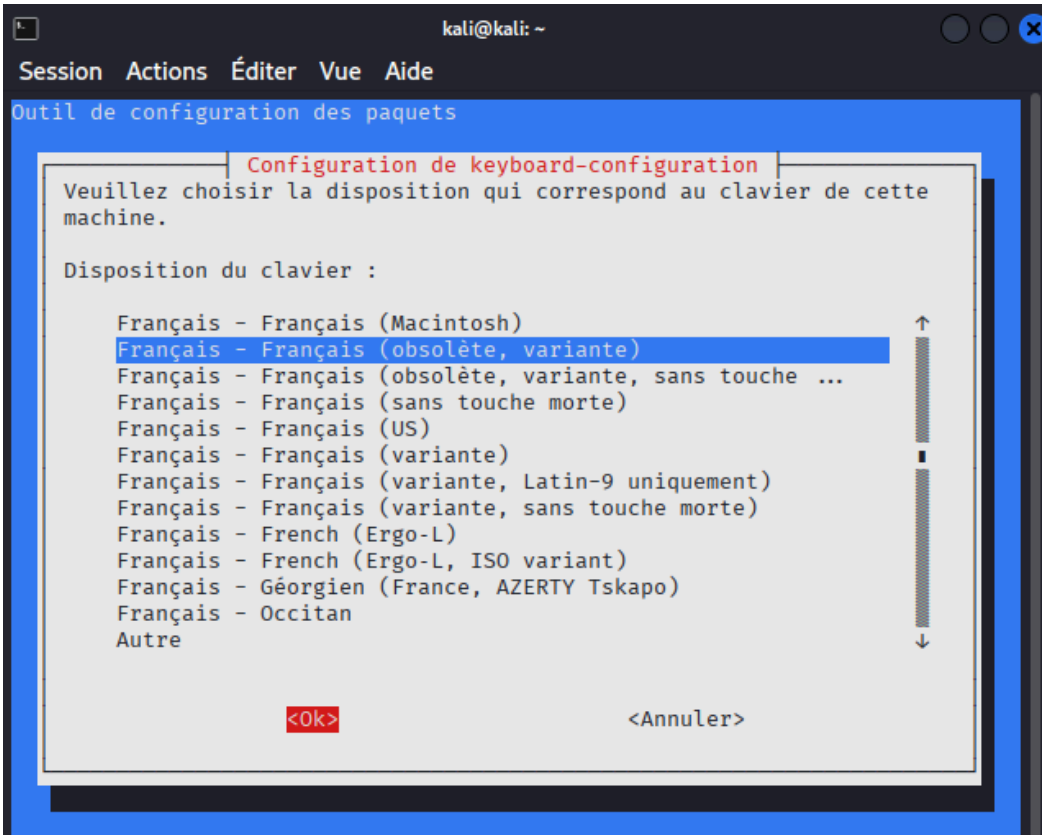

▪ Nous allons mettre le clavier en Français :

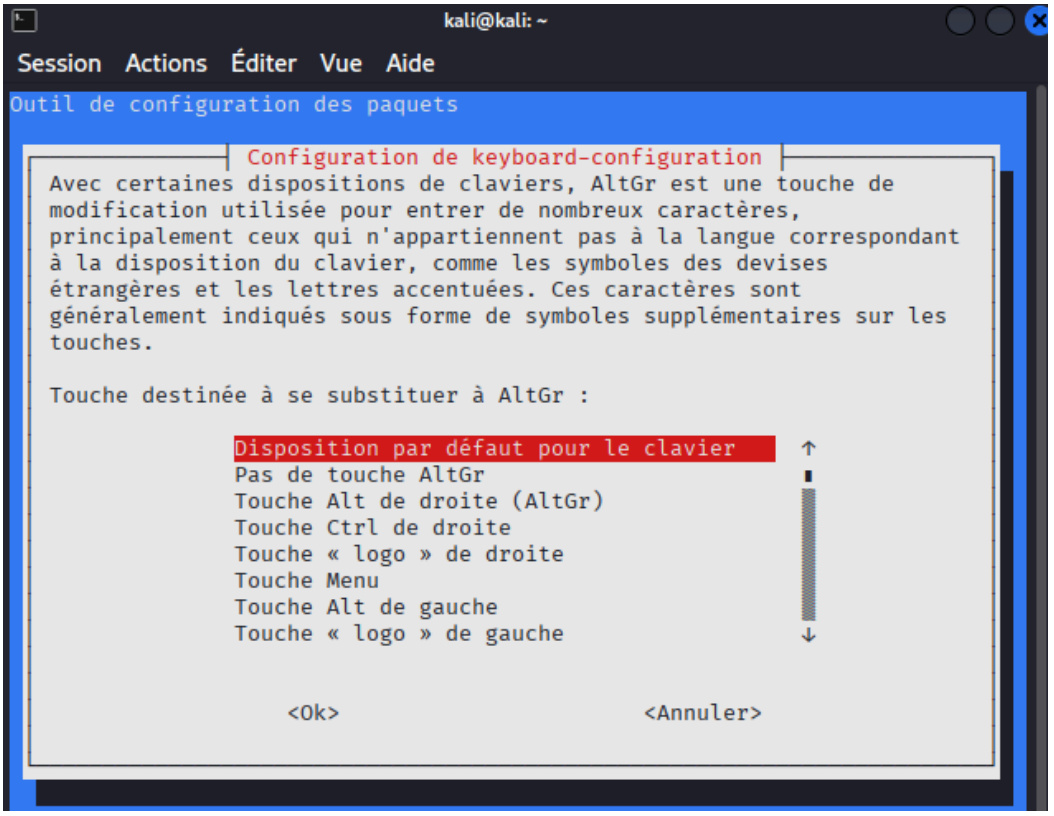


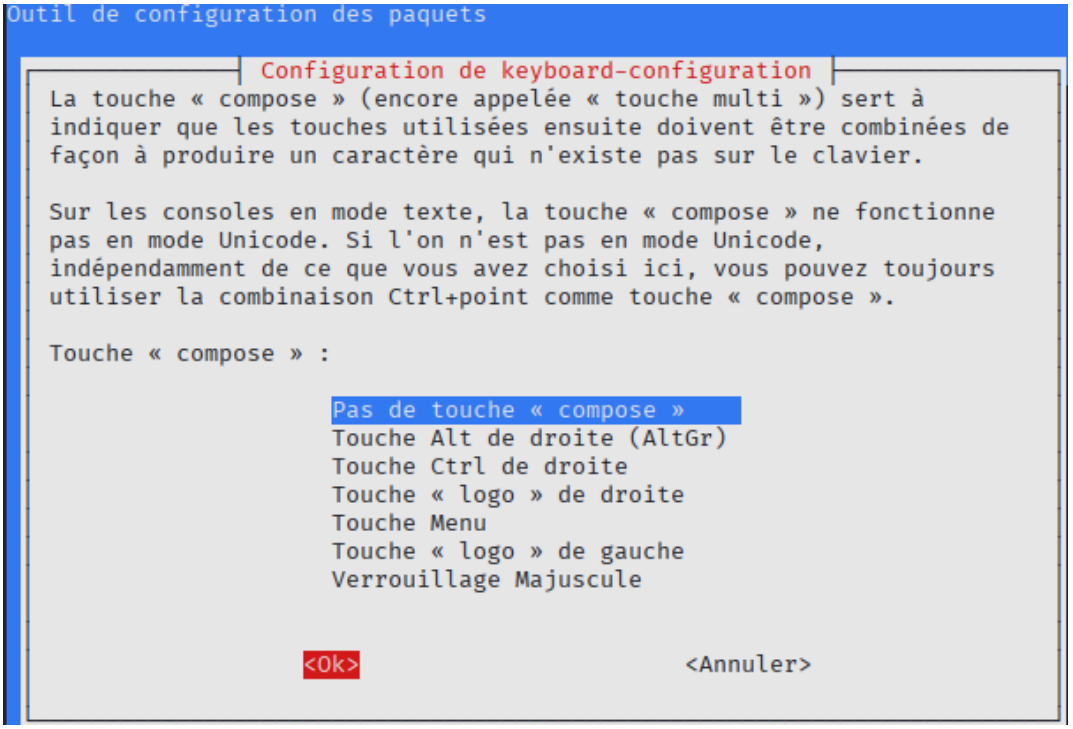

kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
Veuillez choisir le modèle du clavier de cette machine.
Modèle du clavier :
Microsoft Wireless Multimedia 1.0A
NEC SK-1300
NEC SK-2500
NEC SK-6200
NEC SK-7100
Northgate OmniKey 101
OLPC
Ortek MCK-800 Multimédia/Internet
PC-98
PC générique 101 touches
PC générique 102 touches
PC générique 104 touches
PC générique 104 touches avec touche Entrée en L
PC générique 105 touches
<Ok>
<Annuler>

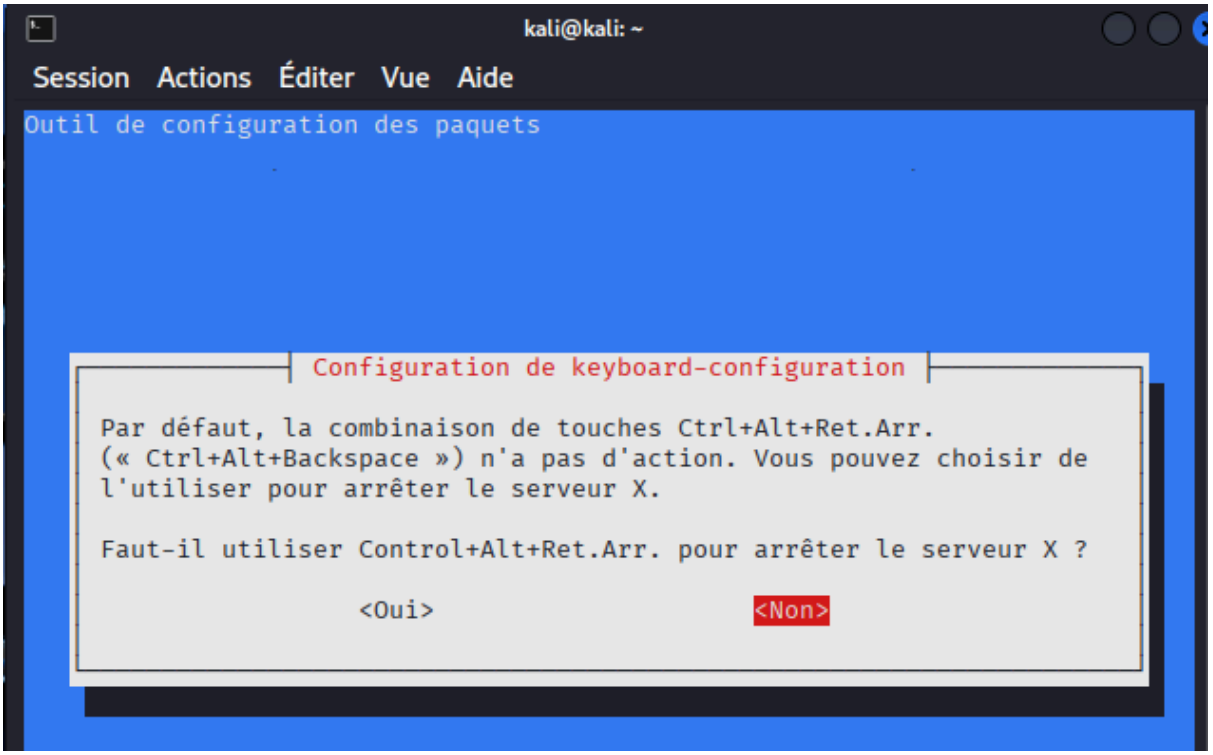

kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
Veuillez choisir la disposition qui correspond au clavier de cette machine.
Disposition du clavier :
Anglais (US) - Anglais (Macintosh)
Anglais (US) - Anglais (Norman)
Anglais (US) - Anglais (US, Euro sur le 5)
Anglais (US) - Anglais (US, internat., avec touches ...
Anglais (US) - Anglais (US, symbolique)
Anglais (US) - Anglais (US, variante internat.)
Anglais (US) - Anglais (Workman)
Anglais (US) - Anglais (Workman, internat., avec ...
Anglais (US) - Cherokee
Anglais (US) - Hawaïen
Anglais (US) - Russe (US, phonétique)
Anglais (US) - Serbo-Croate (US)
Autre
<Ok>
<Annuler>


kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
La disposition des claviers varie selon les pays. Dans certains pays, il peut même exister plusieurs dispositions possibles. Veuillez choisir le pays d'origine du clavier de cette machine.
Pays d'origine du clavier :
Espagnol (Amérique latine)
Espéranto
Estonien
Féroïen
Filipino
Finnois
Français
Français (Canada)
Français (République démocratique du Congo)
Français (Togo)
Géorgien
Grec
<Ok>
<Annuler>

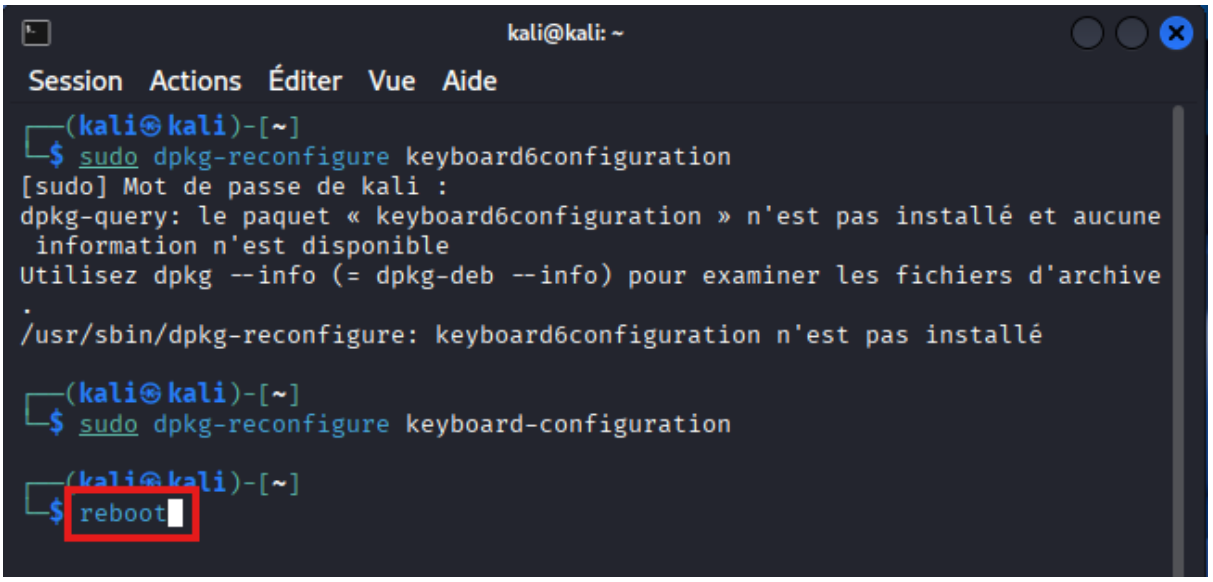

kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
Veuillez choisir la disposition qui correspond au clavier de cette machine.
Disposition du clavier :
Français - Français (Macintosh)
Français - Français (obsolète, variante)
Français - Français (obsolète, variante, sans touche ...
Français - Français (sans touche morte)
Français - Français (US)
Français - Français (variante)
Français - Français (variante, Latin-9 uniquement)
Français - Français (variante, sans touche morte)
Français - French (Ergo-L)
Français - French (Ergo-L, ISO variant)
Français - Géorgien (France, AZERTY Tskapo)
Français - Occitan
Autre
<Ok>
<Annuler>


kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
Avec certaines dispositions de claviers, AltGr est une touche de modification utilisée pour entrer de nombreux caractères, principalement ceux qui n'appartiennent pas à la langue correspondant à la disposition du clavier, comme les symboles des devises étrangères et les lettres accentuées. Ces caractères sont généralement indiqués sous forme de symboles supplémentaires sur les touches.
Touche destinée à se substituer à AltGr :
Disposition par défaut pour le clavier
Pas de touche AltGr
Touche Alt de droite (AltGr)
Touche Ctrl de droite
Touche « logo » de droite
Touche Menu
Touche Alt de gauche
Touche « logo » de gauche
<Ok>
<Annuler>

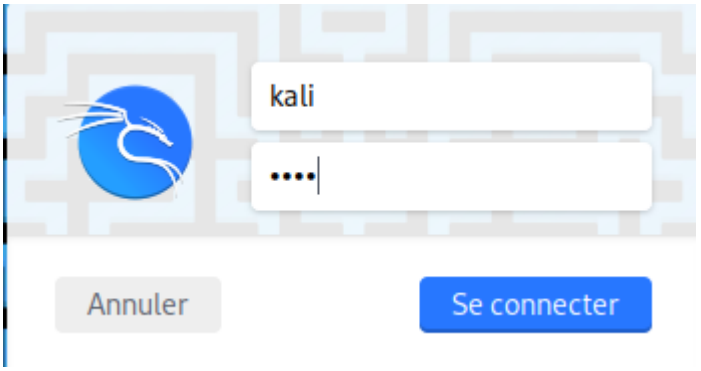

Outil de configuration des paquets
Configuration de keyboard-configuration
La touche « compose » (encore appelée « touche multi ») sert à
indiquer que les touches utilisées ensuite doivent être combinées de
façon à produire un caractère qui n'existe pas sur le clavier.
Sur les consoles en mode texte, la touche « compose » ne fonctionne
pas en mode Unicode. Si l'on n'est pas en mode Unicode,
indépendamment de ce que vous avez choisi ici, vous pouvez toujours
utiliser la combinaison Ctrl+point comme touche « compose ».
Touche « compose » :
Pas de touche « compose »
Touche Alt de droite (AltGr)
Touche Ctrl de droite
Touche « logo » de droite
Touche Menu
Touche « logo » de gauche
Verrouillage Majuscule
<Ok>
<Annuler>


kali@kali: ~
Session Actions Éditer Vue Aide
Outil de configuration des paquets
Configuration de keyboard-configuration
Par défaut, la combinaison de touches Ctrl+Alt+Ret.Arr.
(« Ctrl+Alt+Backspace ») n'a pas d'action. Vous pouvez choisir de
l'utiliser pour arrêter le serveur X.
Faut-il utiliser Control+Alt+Ret.Arr. pour arrêter le serveur X ?
<Oui>
<Non>

▪ Nous procédons par un redémarrage de la VM




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



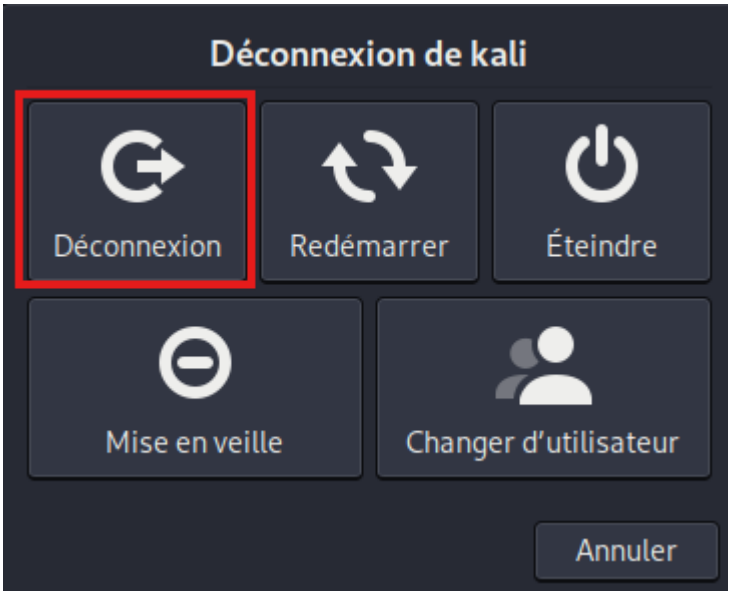
▪ Nous allons activer le compte root :
Tout d'abord nous allons procéder par un  (apt-get update avant)

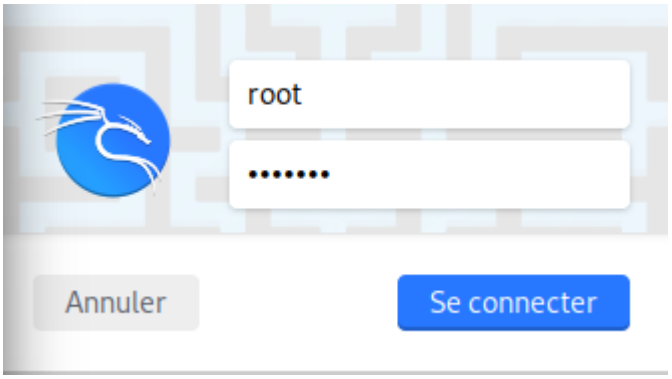
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] Mot de passe de kali :
Réception de : 1 http://archive-4.kali.org/kali kali-rolling InRelease [34,0
kB]
Réception de : 2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packa
ges [20,9 MB]
Réception de : 3 http://archive-4.kali.org/kali kali-rolling/main 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
```

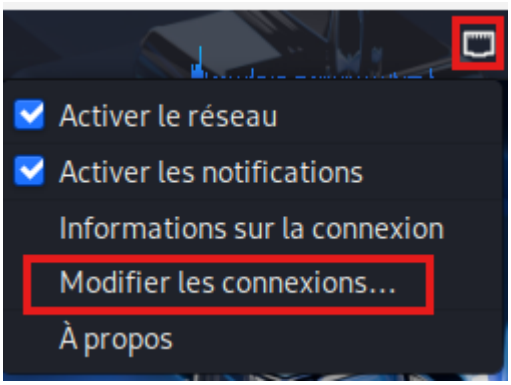
Mot de passe de root : Azerty0

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

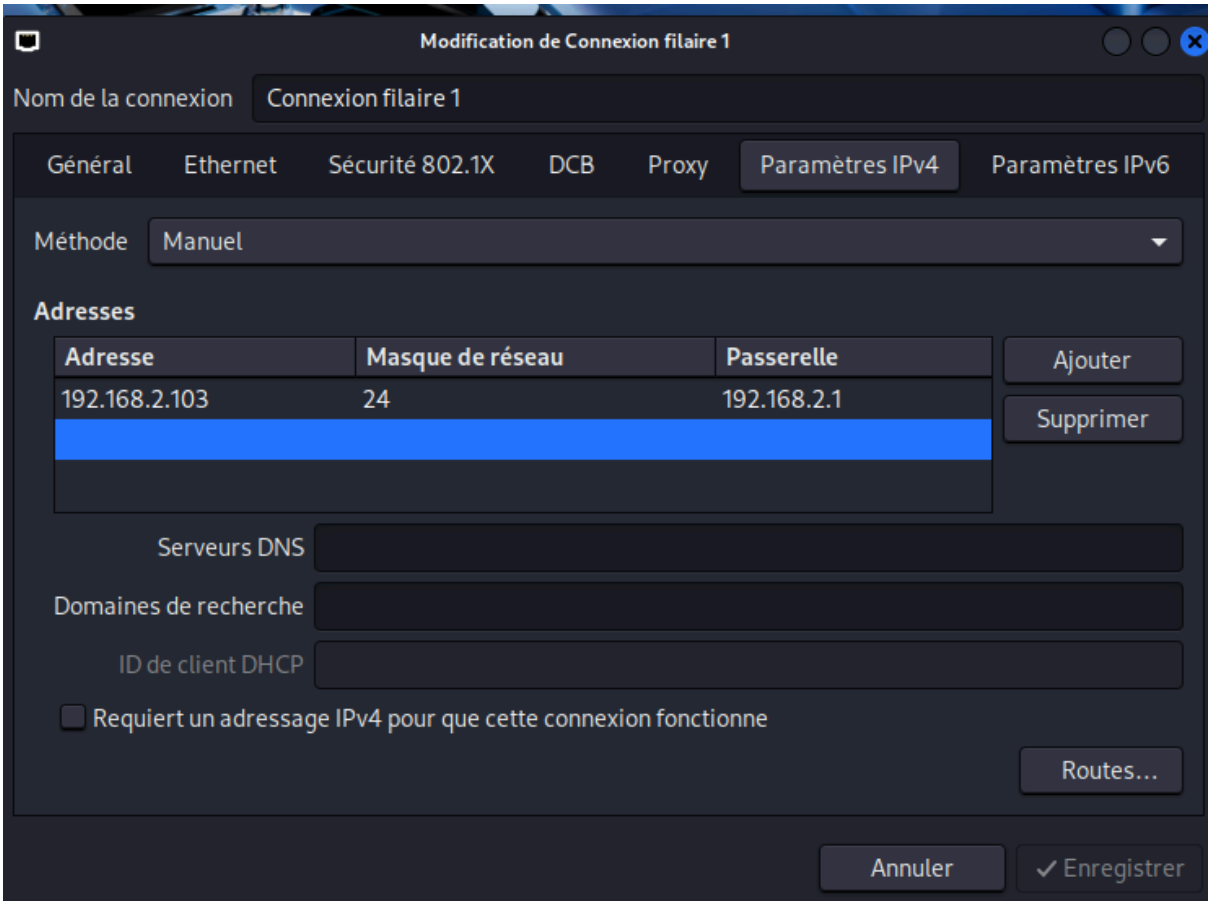


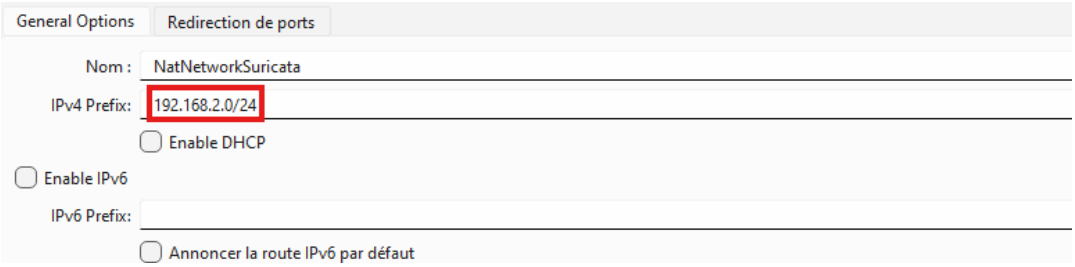
▪ Configuration des propriétés IPv4 de la carte réseau : cliquer droit sur l'icône Connexion réseau.

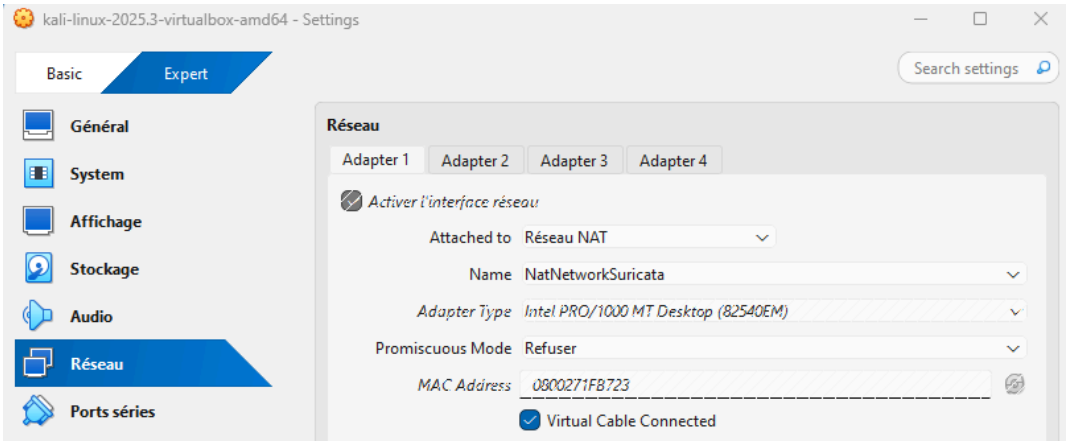



Ne pas oublier la passerelle.

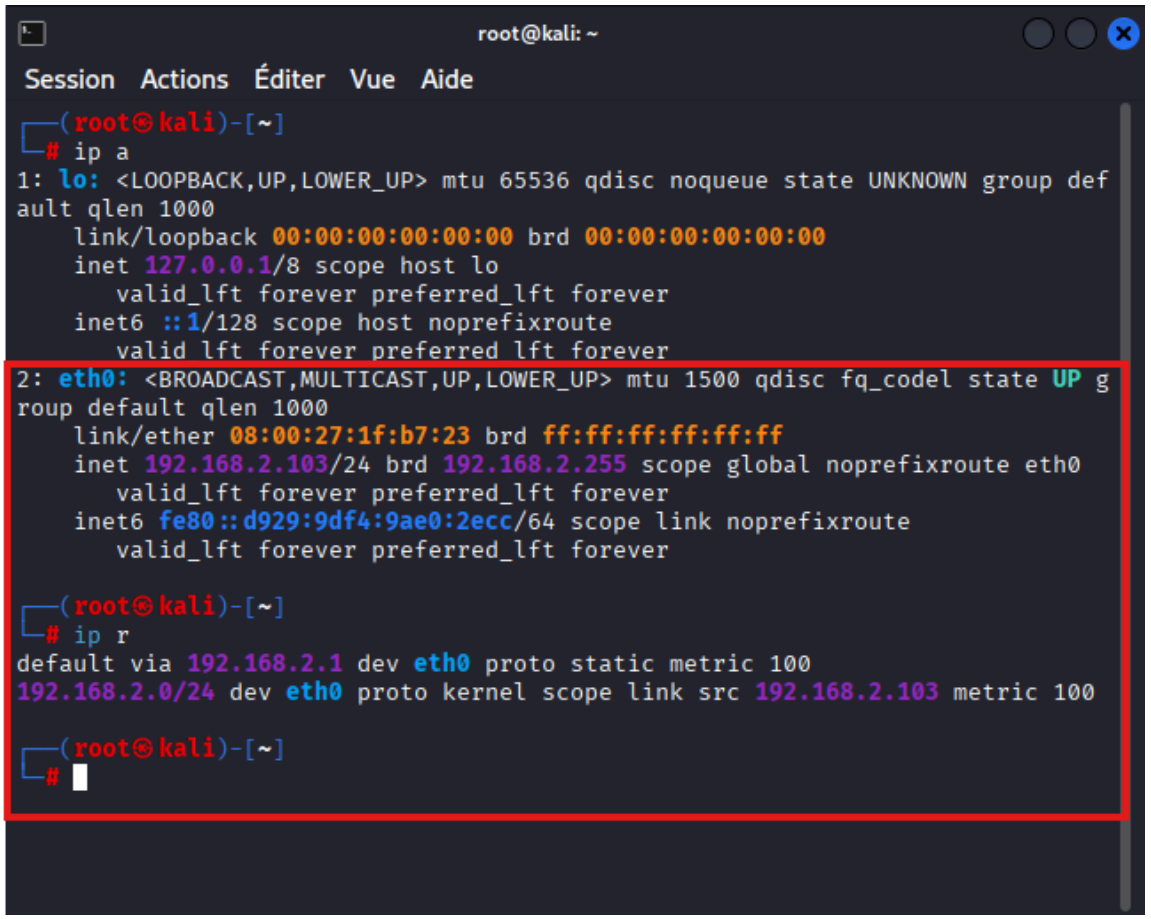


▪ Création d'un réseau NAT appelé NatNetworkSuricata (192.168.2.0/24) et nous modifions le mode d'accès réseau de la VM :



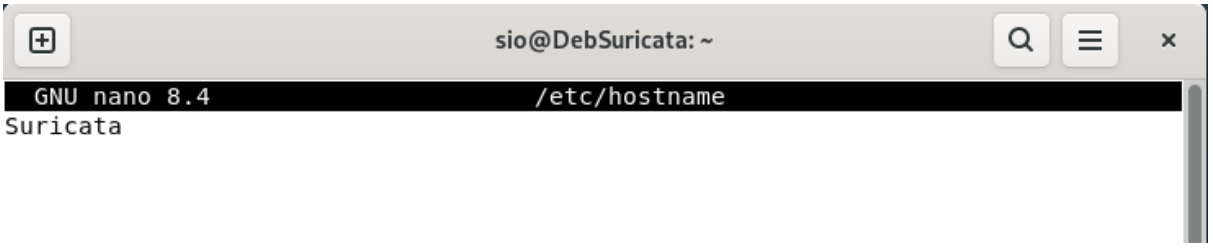

▪ Nous vérifions les paramètres :



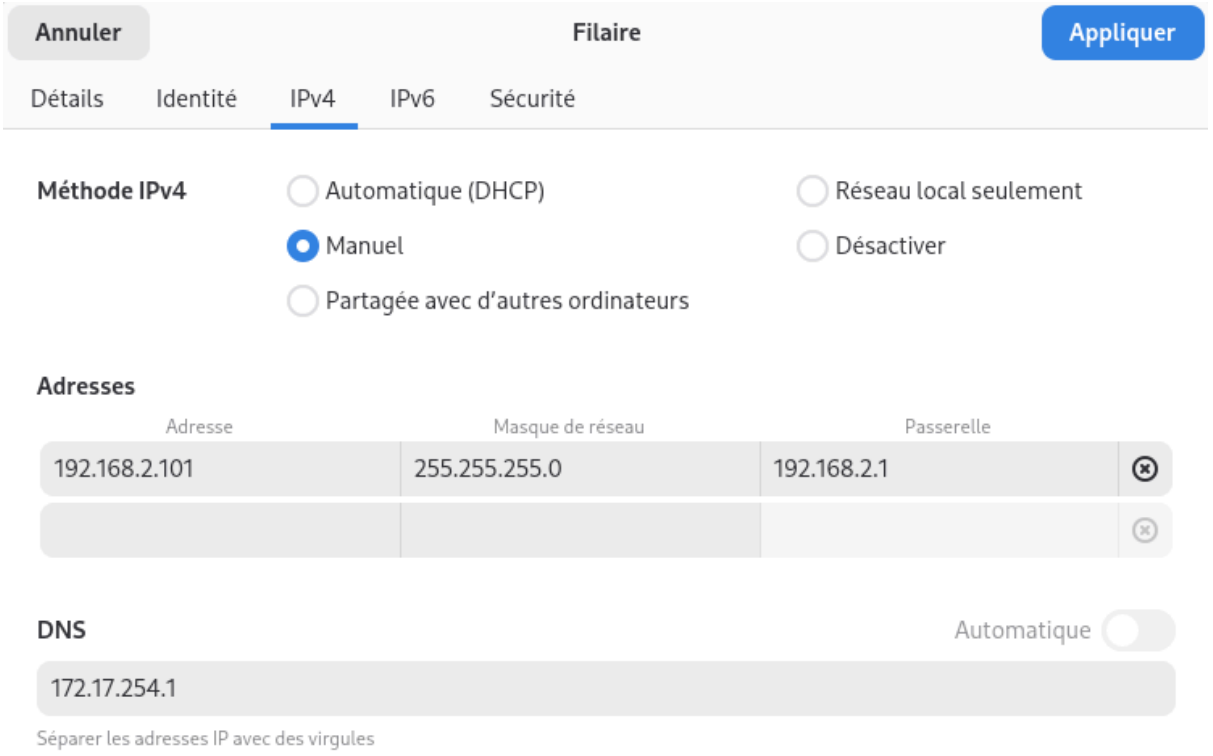
# 2) VM Suricata : installer Suricata et jq (json query).

▪ Configuration de la carte réseau.
Fait

▪ Nous modifions les fichiers /etc/hosts et /etc/hosname puis nous effectuons un reboot pour appliquer les changements







- Faire un apt-get update et installer suricata :

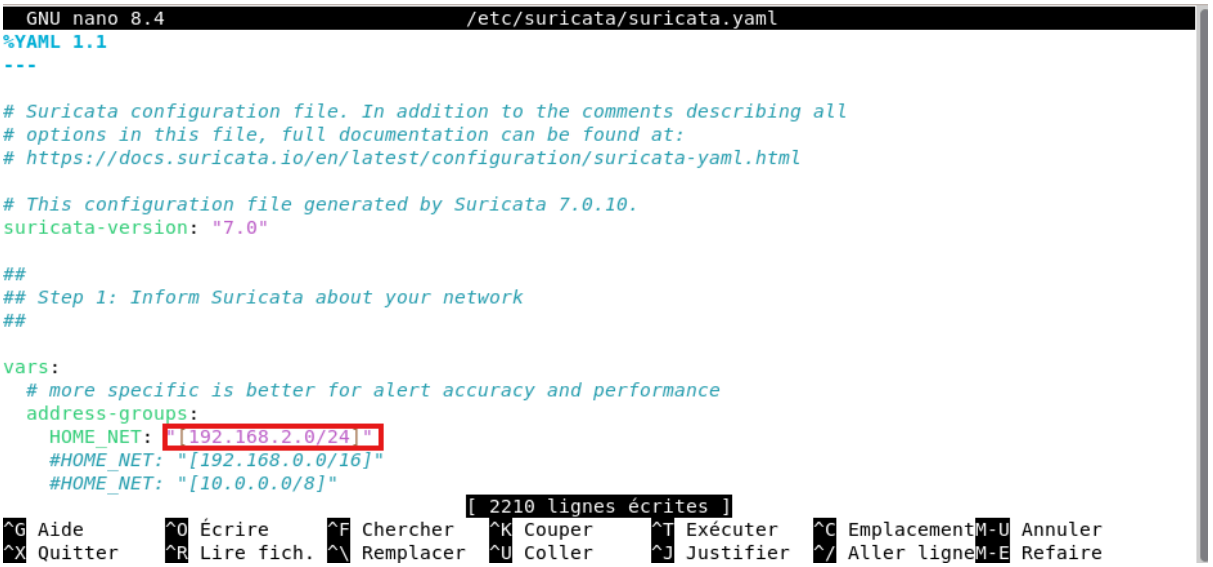
```
root@Suricata:~# apt-get update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://deb.debian.org/debian trixie-updates InRelease
Réception de : 3 http://security.debian.org/debian-security trixie-security InRelease [43,4 kB]
43,4 ko réceptionnés en 0s (141 ko/s)
Lecture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

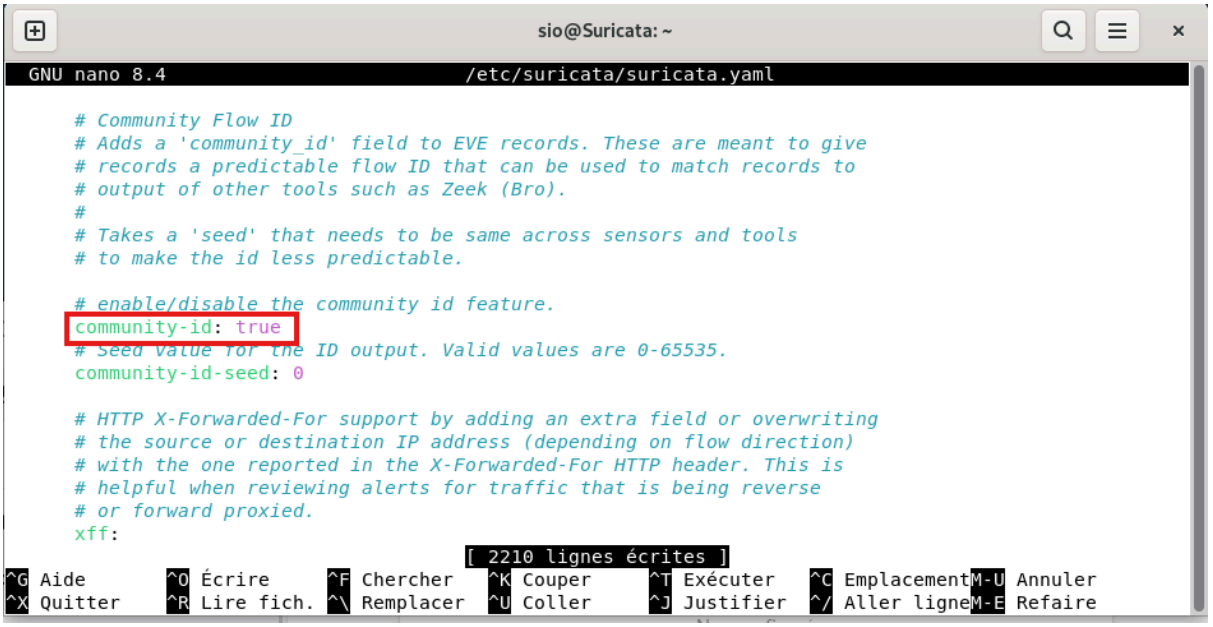
```
root@Suricata:~# apt-get install suricata jq
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
jq est déjà la version la plus récente (1.7.1-6+deb13u1).
jq passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  isa-support libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0 libhtp2
  libhyperscan5 libluajit-5.1-2 libluajit-5.1-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 libhtp2
```

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

##
## 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. ^\ 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. ^\ 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 :

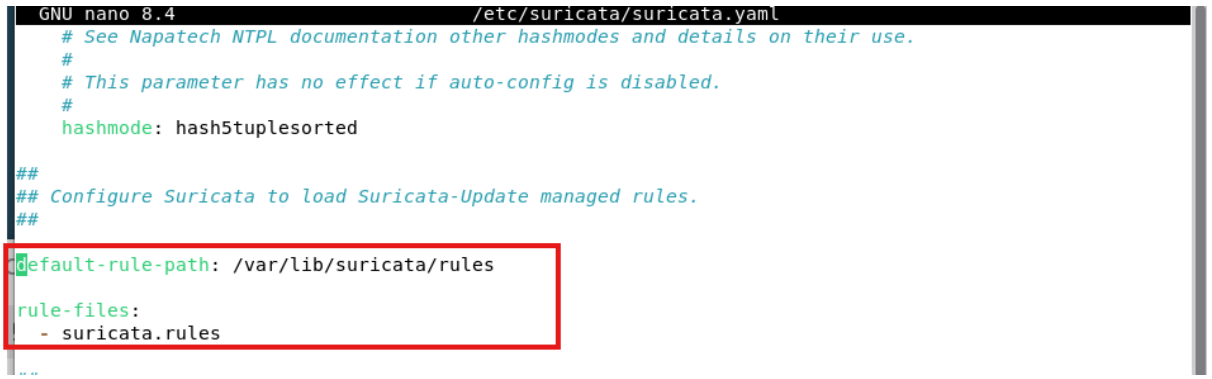
```
root@Suricata:~# systemctl start suricata
root@Suricata:~# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-10-16 12:30:00 CEST; 7s ago
 Invocation: d9fe87263da9420f9ec0a4eabbc1a167
       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 :

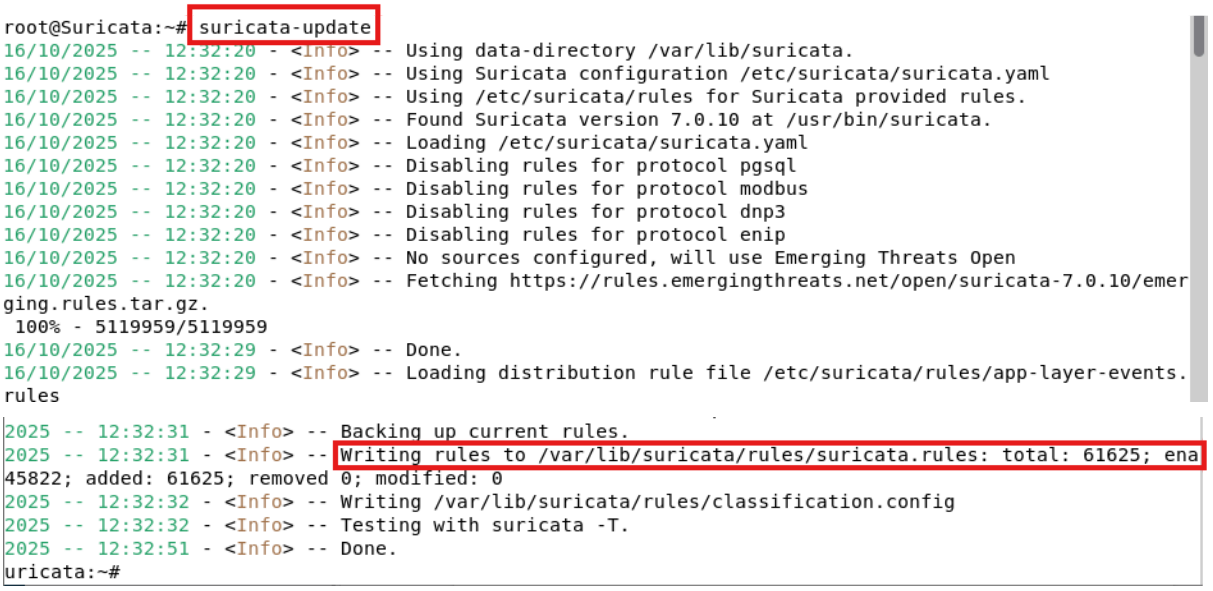
```
root@Suricata:~# systemcrl enable suricata
-bash: systemcrl : commande introuvable
root@Suricata:~# systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-ins
tall.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata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

# 4) Importer les règles Emerging Threat Open

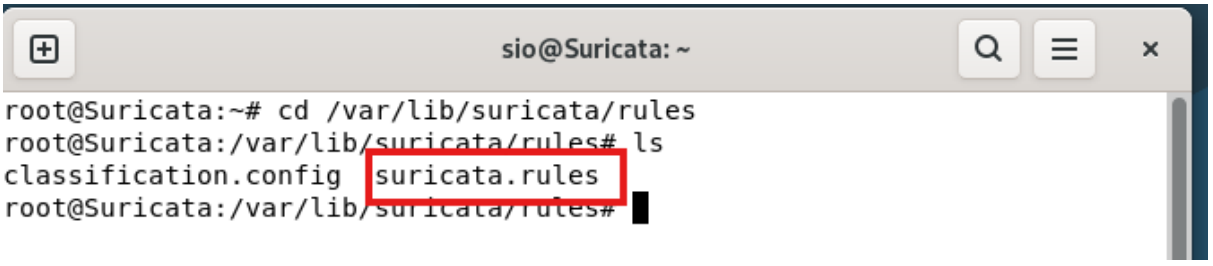
▪ Nous consultons l'emplacement et le nom du fichier des règles spécifié dans le fichier de configuration :




▪ 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 :




▪ Nous vérifions la présence du fichier 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: ~
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) initiali
zed: eve.json
[4327 - Suricata-Main] 2025-10-16 12:38:21 Info: logopenfile: stats output device (regular) initialize
d: stats.log
[4327 - Suricata-Main] 2025-10-16 12:38:28 Info: detect: 1 rule files processed. 45822 rules successfu
lly 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 r
ules, 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 recomme
nded 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   Engi
ne started.
```

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

▪ Installation de curl :

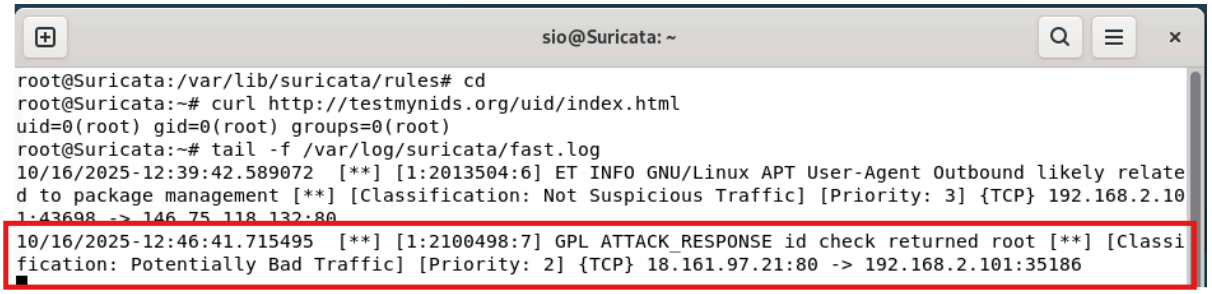
```
sio@Suricata: ~
root@Suricata:~# apt-get install curl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  curl
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non 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) :

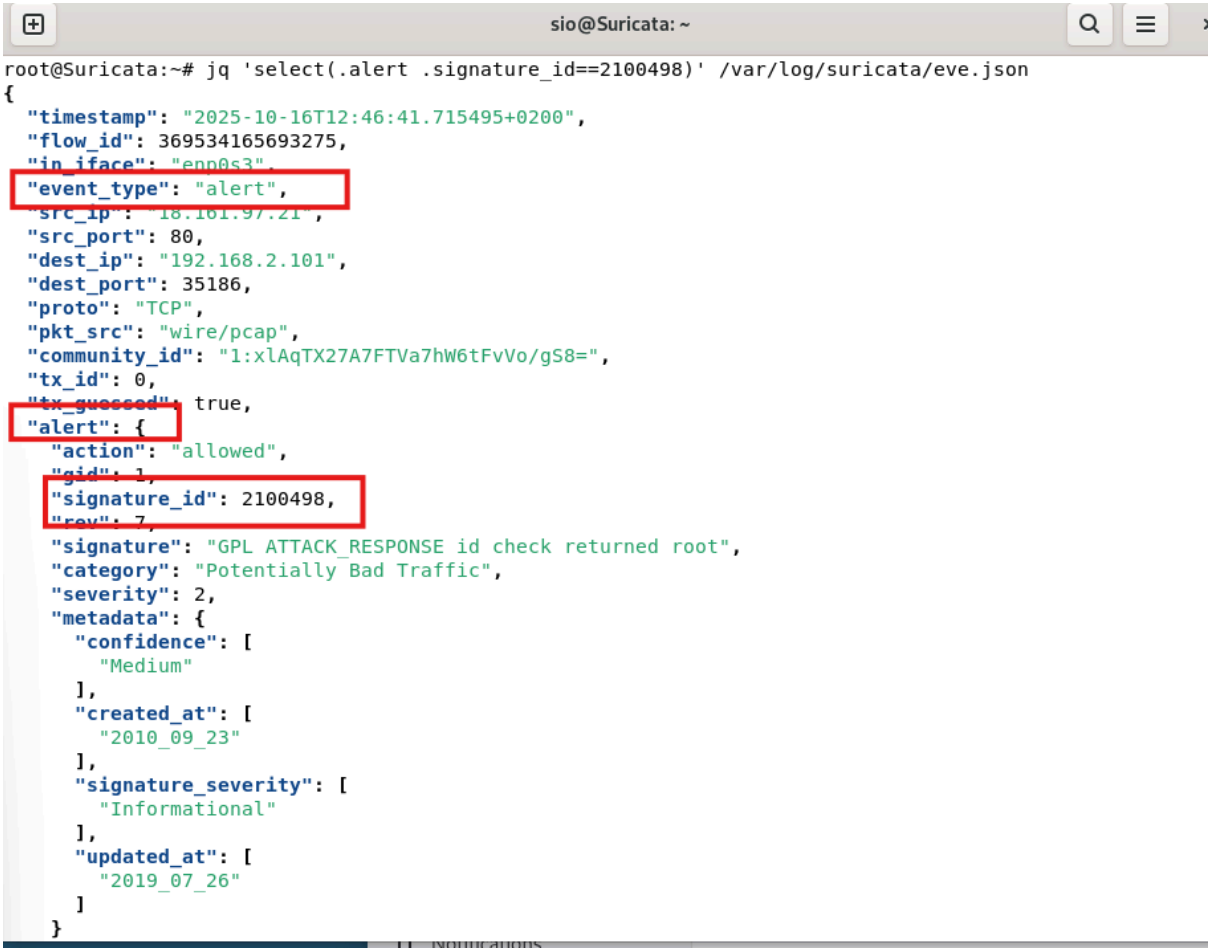
```
 GNU nano 8.4                                    suricata.rules
# alert dns $HOME_NET any -> any any (msg:"ET ADWARE_PUP DNS Query to CoinMiner Proxy Domain (xmrminingproxy
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ADWARE_PUP Onestart AI Host Profile Checkin (POST)"; f
alert http $HOME_NET 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
```

```
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:~#
```

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

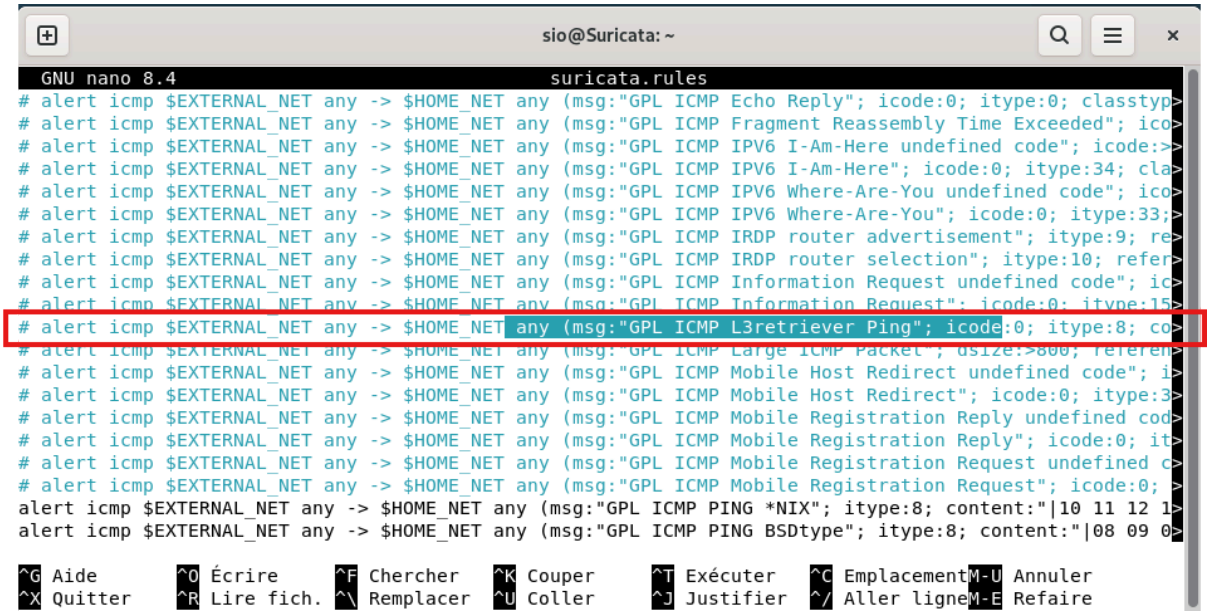



▪ Nous vérifions la présence de l'alerte dans le log eve au format json avec la commande jq (permet d'extraire et de lire des données json) :

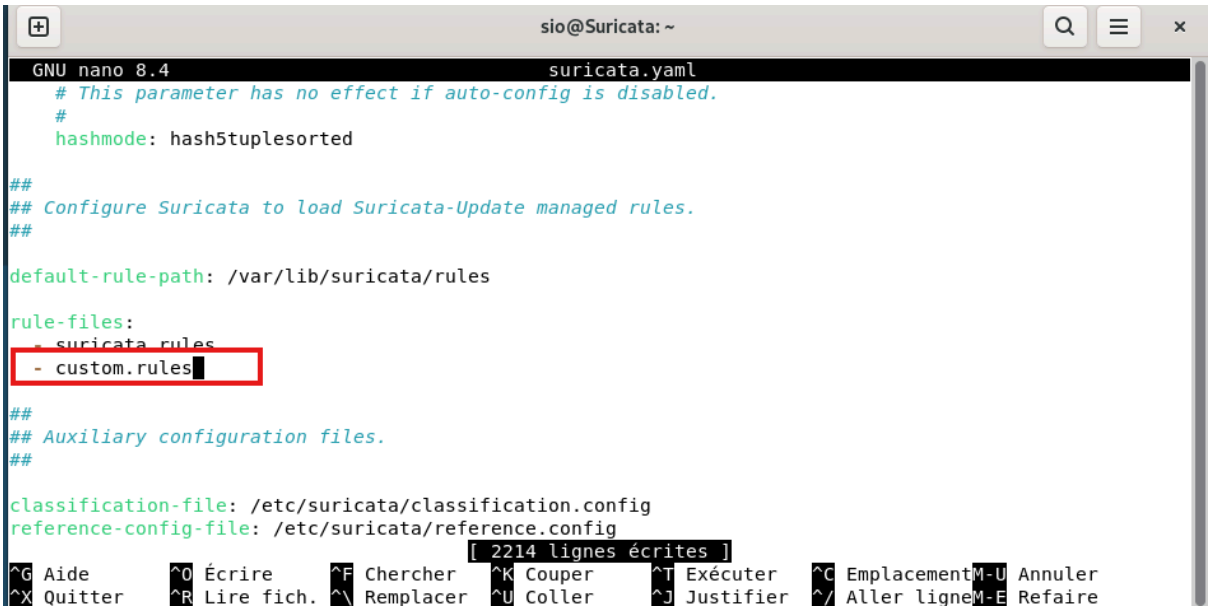


# 6) Créer 2 règles personnalisées :

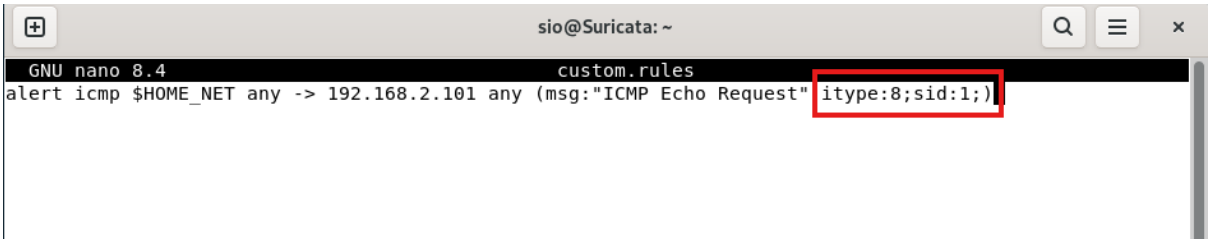
▪ Consulter une règle ICMP du fichier suricata.rules (recherche ctrl + F dans Nano avec itype:8). Etudier de nouveau sa construction. On constate qu'elle est commentée :

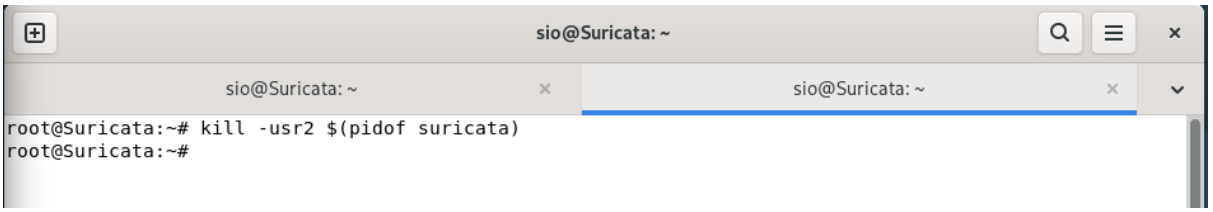



▪ Spécification d'un fichier pour nos propres règles dans le fichier de configuration suricata.yaml :

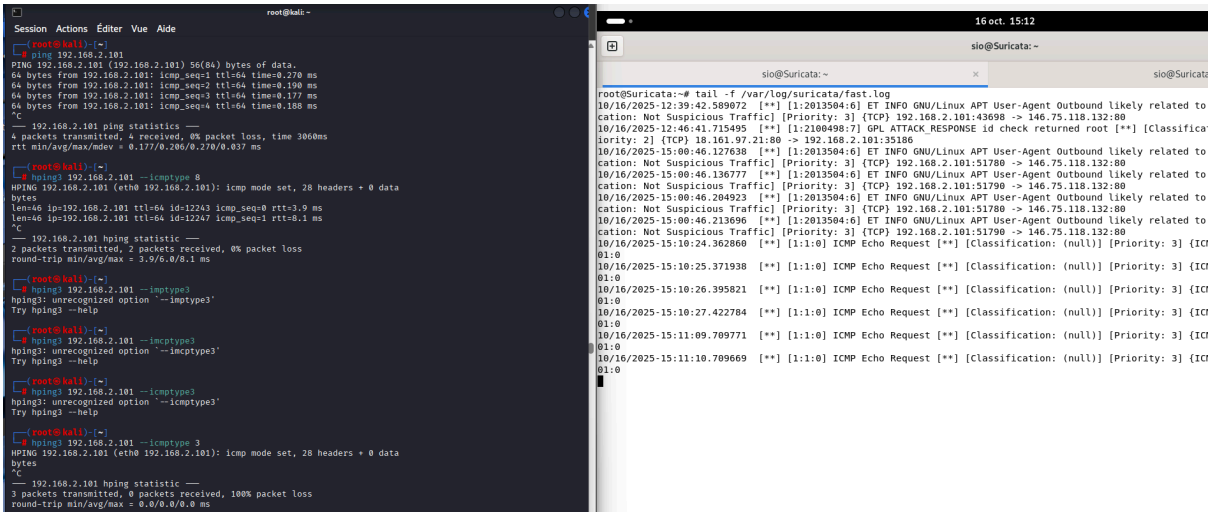


▪ Nous créons une règle pour déclencher une alerte suite à la réception d'une requête ICMP type 8 :



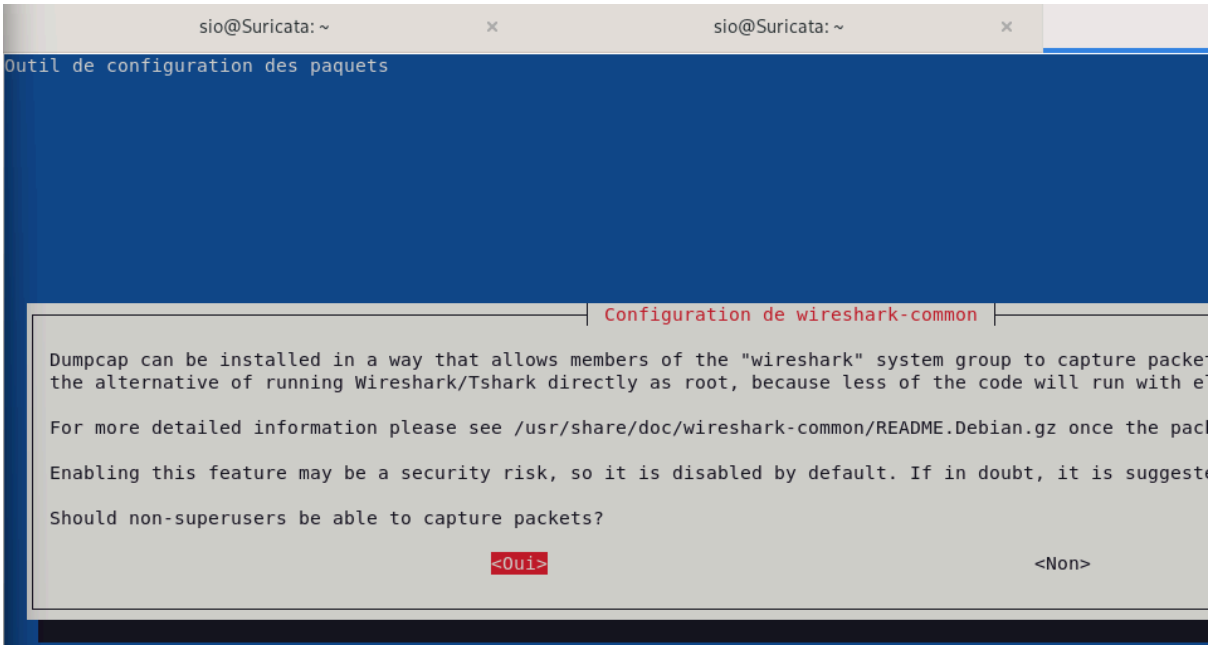



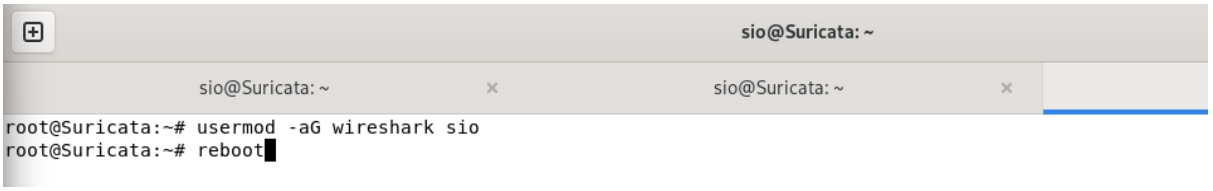

▪ Test de la règle avec les commandes ping, hping3 puis nmap depuis la VM Kali

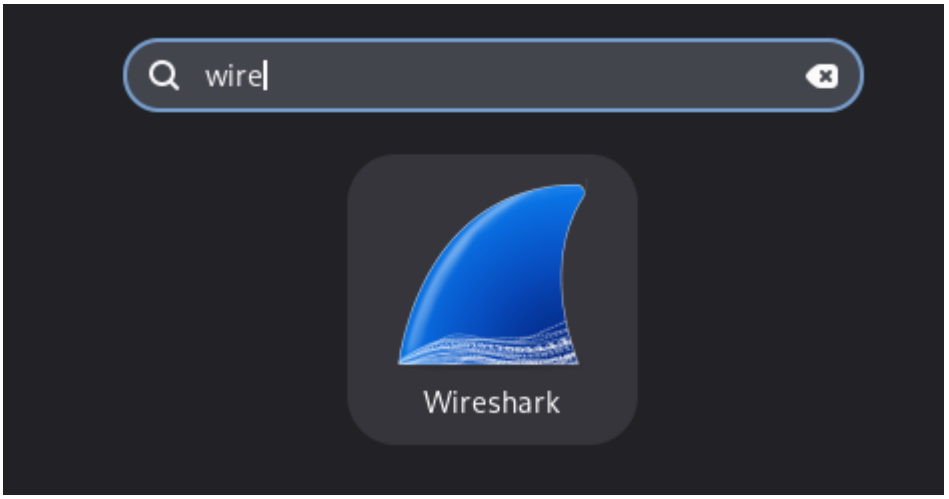


Nous effectuons un apt-get update et apt-get install wireshark :

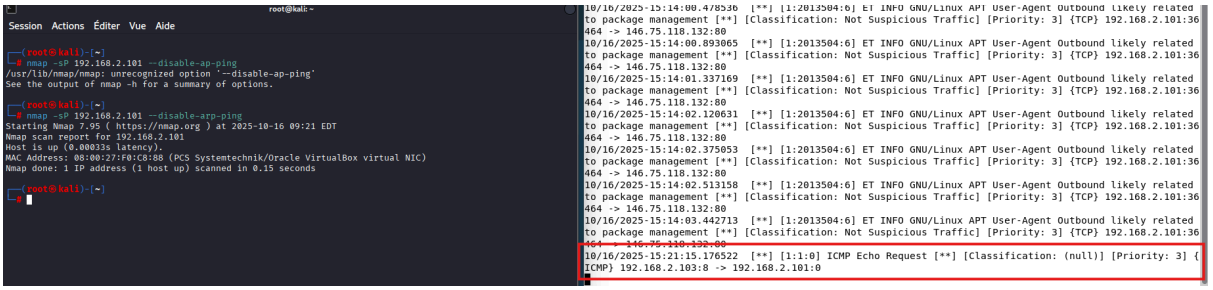
```
sio@Suricata:~$ su - root
Mot de passe :
root@Suricata:~# apt-get update
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Lecture des listes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

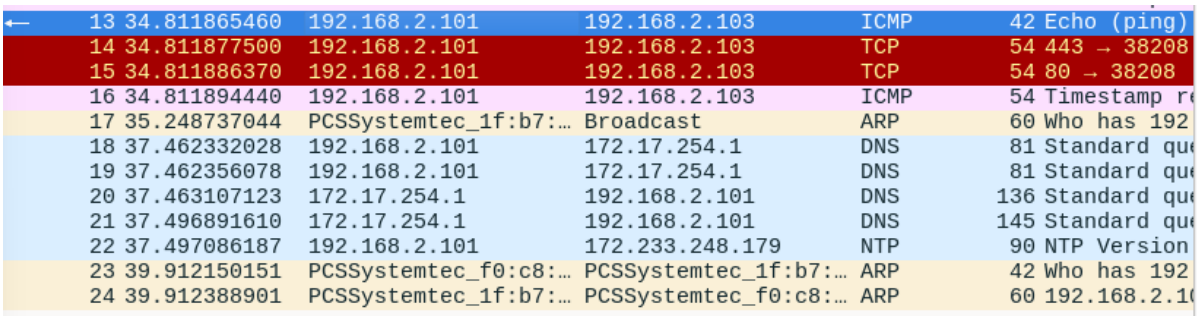


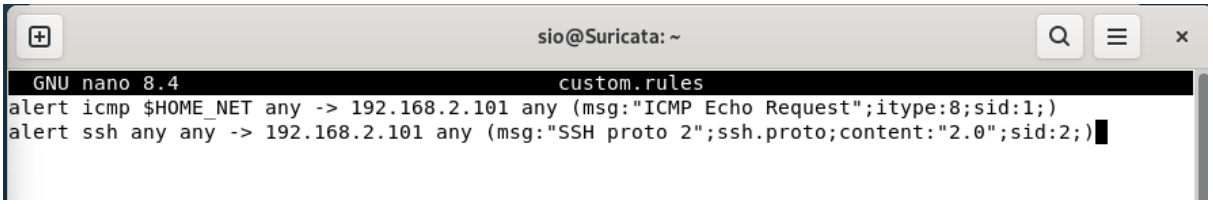



▪ Nous lançons une capture avant commande nmap depuis Kali

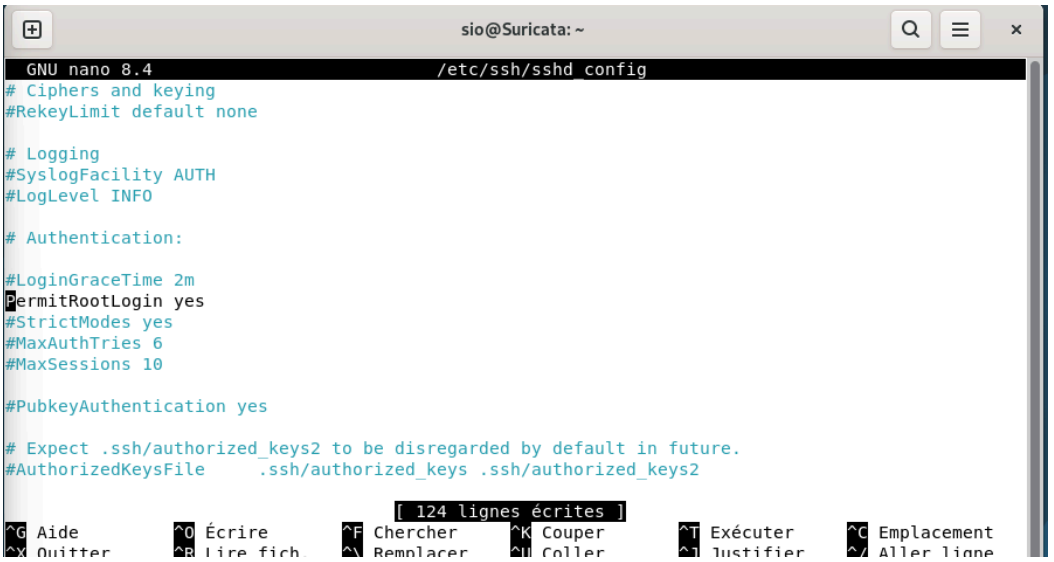


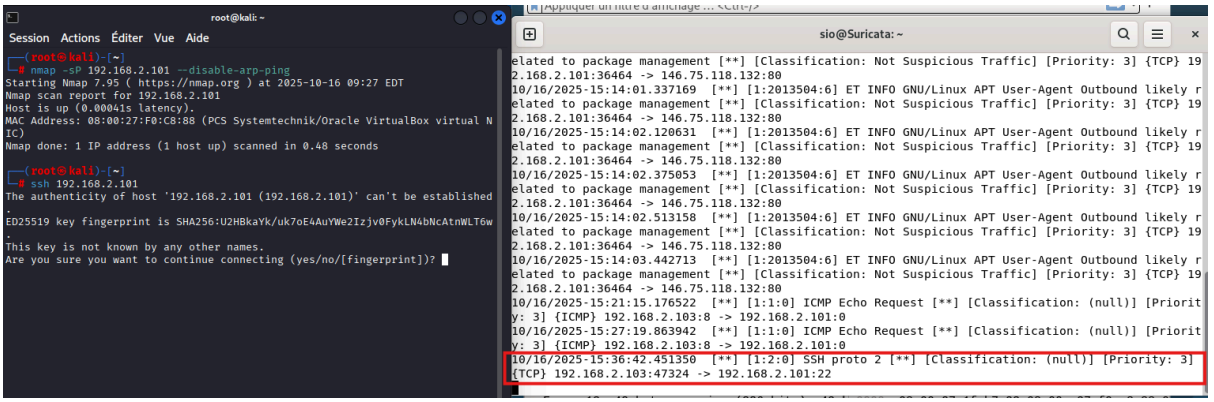




▪ Nous créons une seconde règle, destinée à déclencher une alerte suite à un flux SSH, à l'aide des keyword ssh.proto et content.




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

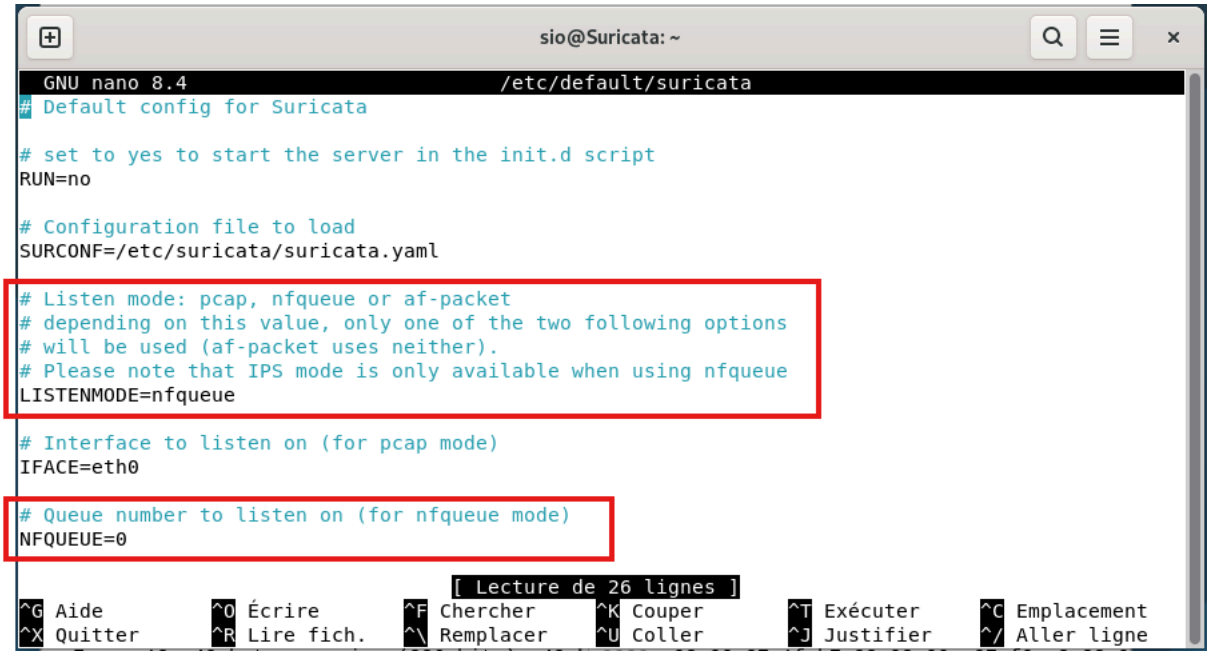


# 7) Basculer Suricata en mode IPS :

## a) Configuration de Suricata :

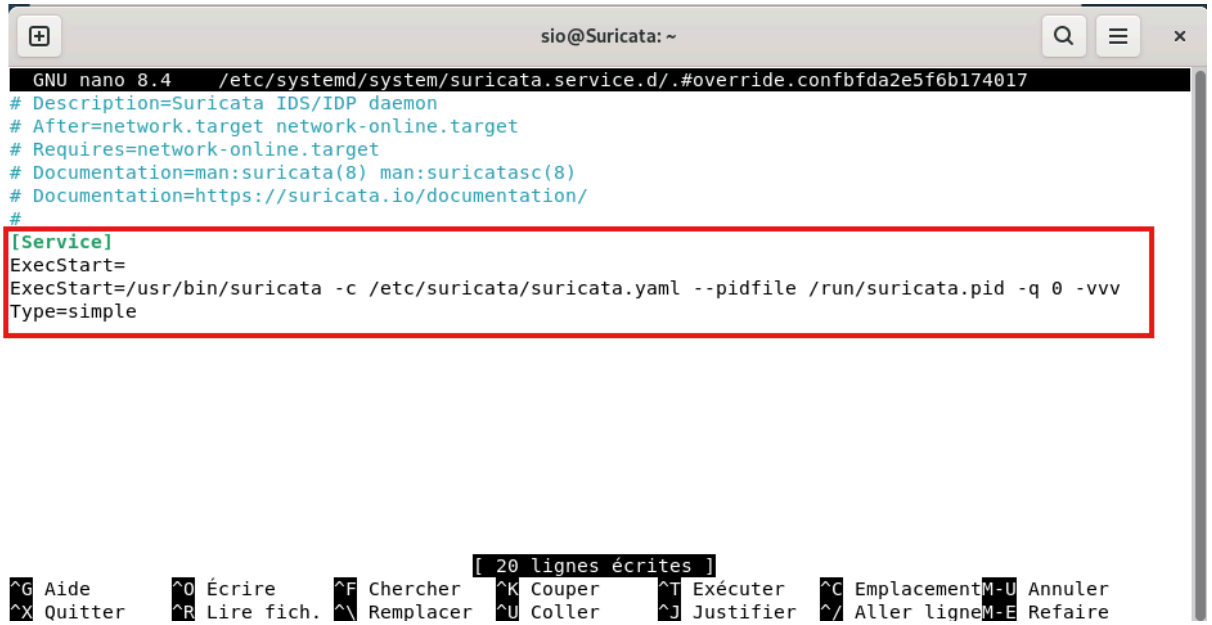
▪ Nous vérifions dans le fichier /etc/default/suricata que la directive LISTENMODE soit déjà égale à nfqueue et non pas à af-packet :



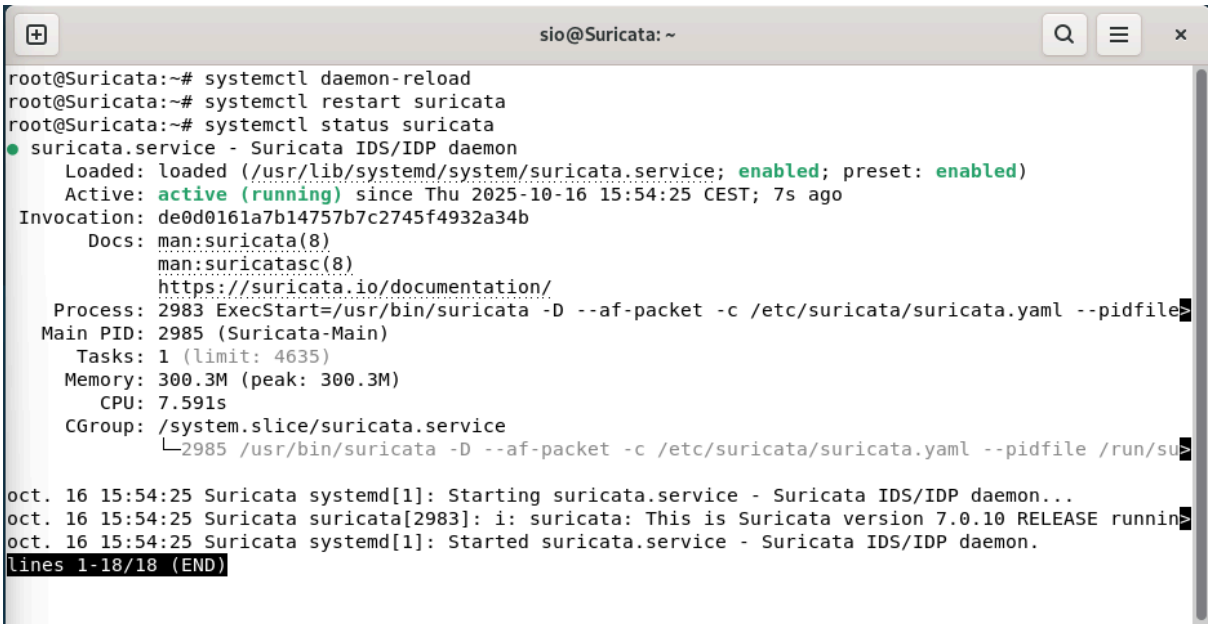

▪ Pour activer le mode nfqueue manuellement (à saisir à nouveau au prochain redémarrage du serveur) :

```
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

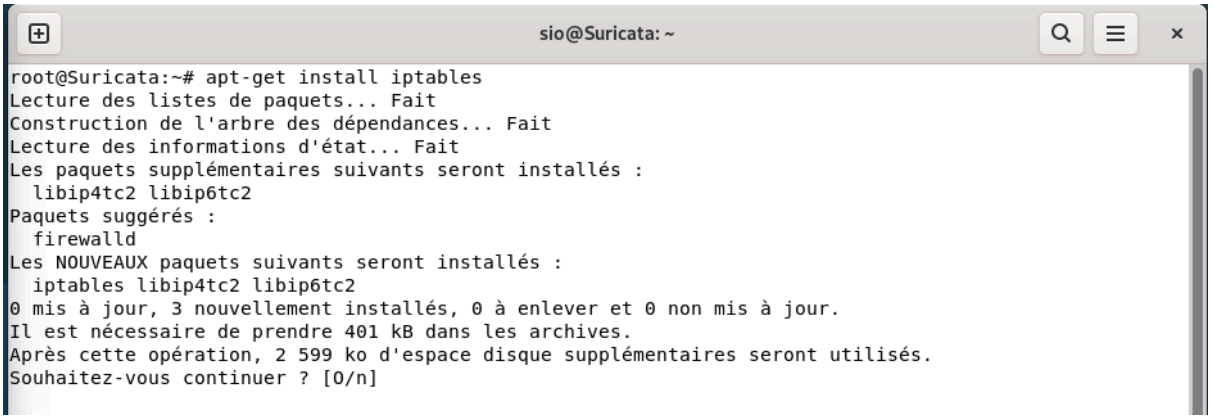


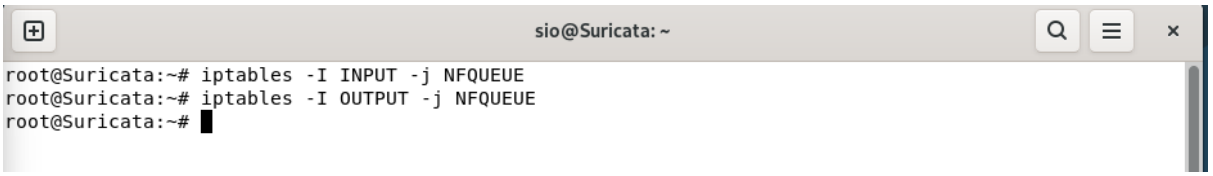

▪ Nous rechargeons systemd puis nous redémarrons suricata et pour ainsi vérifier son état :



# b) Configurer IPtables (NFQUEUE)

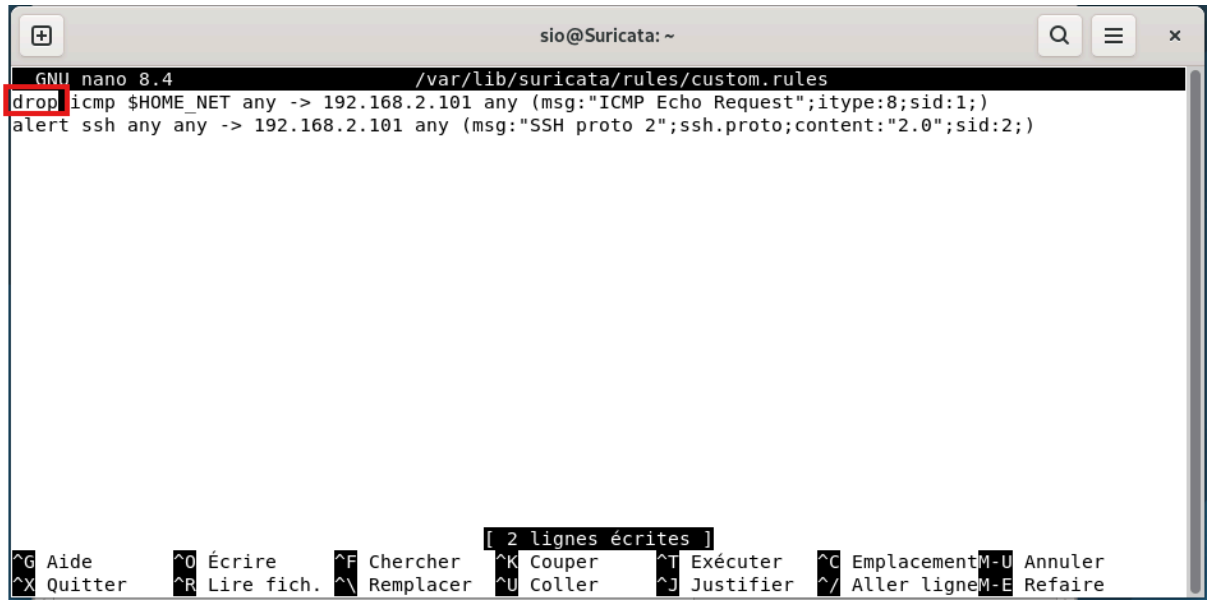
- Nous effectuons apt-get install iptables

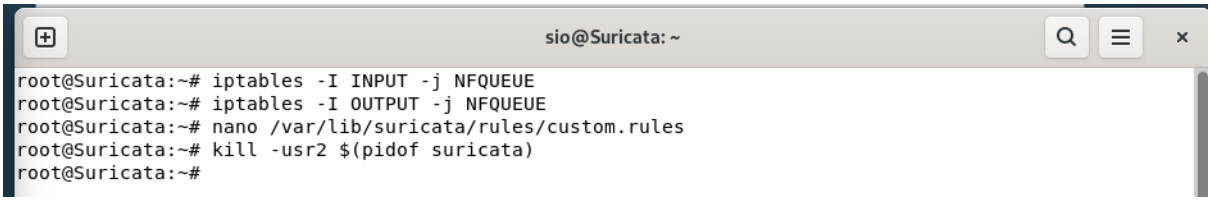


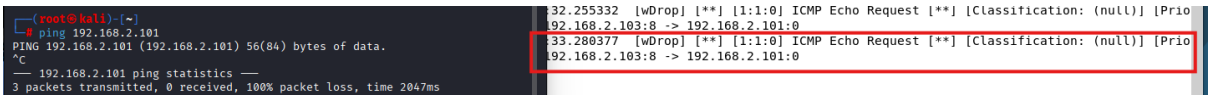
# 8) Test du bon fonctionnement du mode IPS :

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

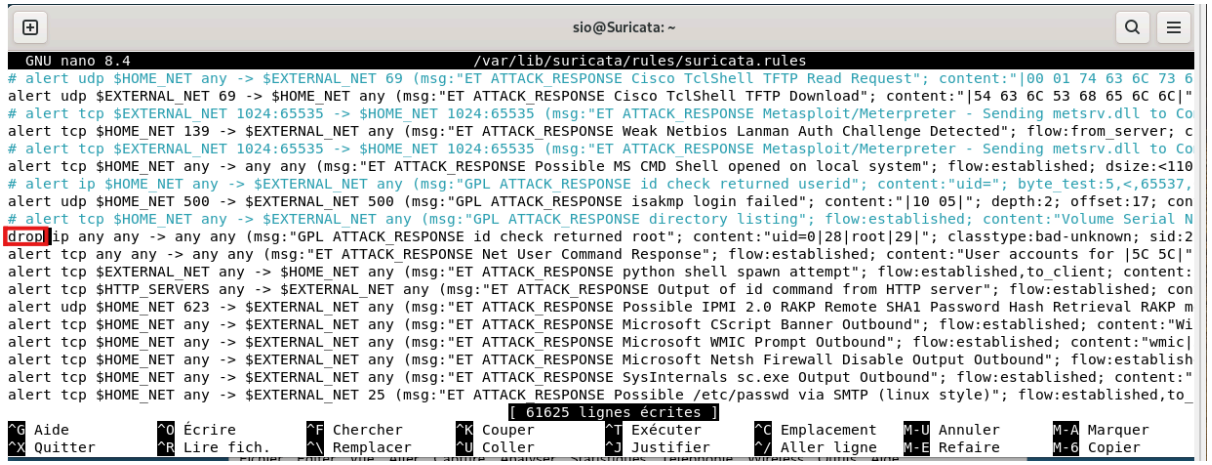


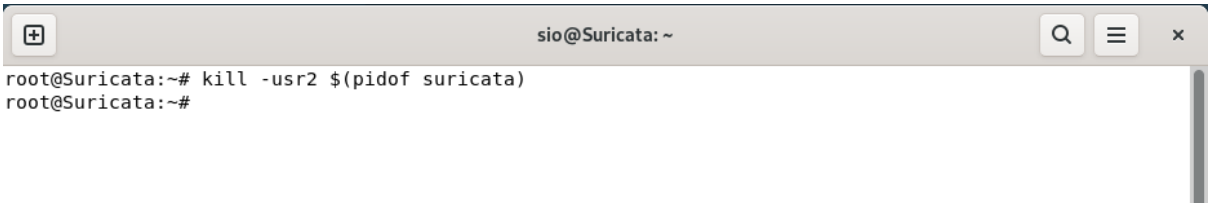




▪ Nous effectuons un ping depuis Kali et nous vérifions dans le log fast.log que l'action Drop a bien été effectuée par Suricata :

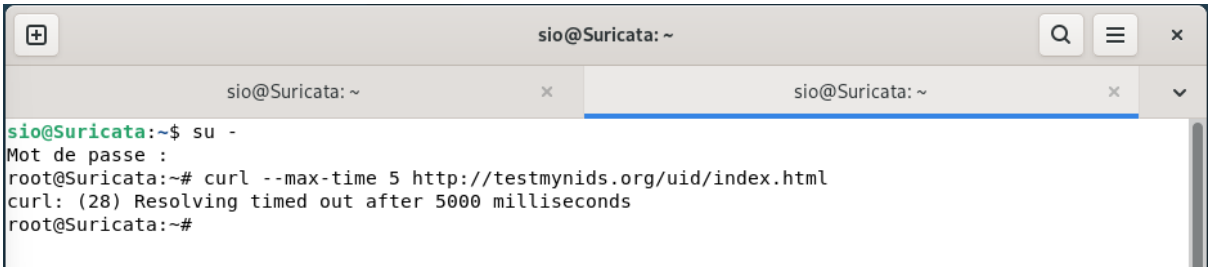


▪ Modification dans le fichier suricata.rules l'action de la règle dont le sid est 2100498 (cf. test page 21) :

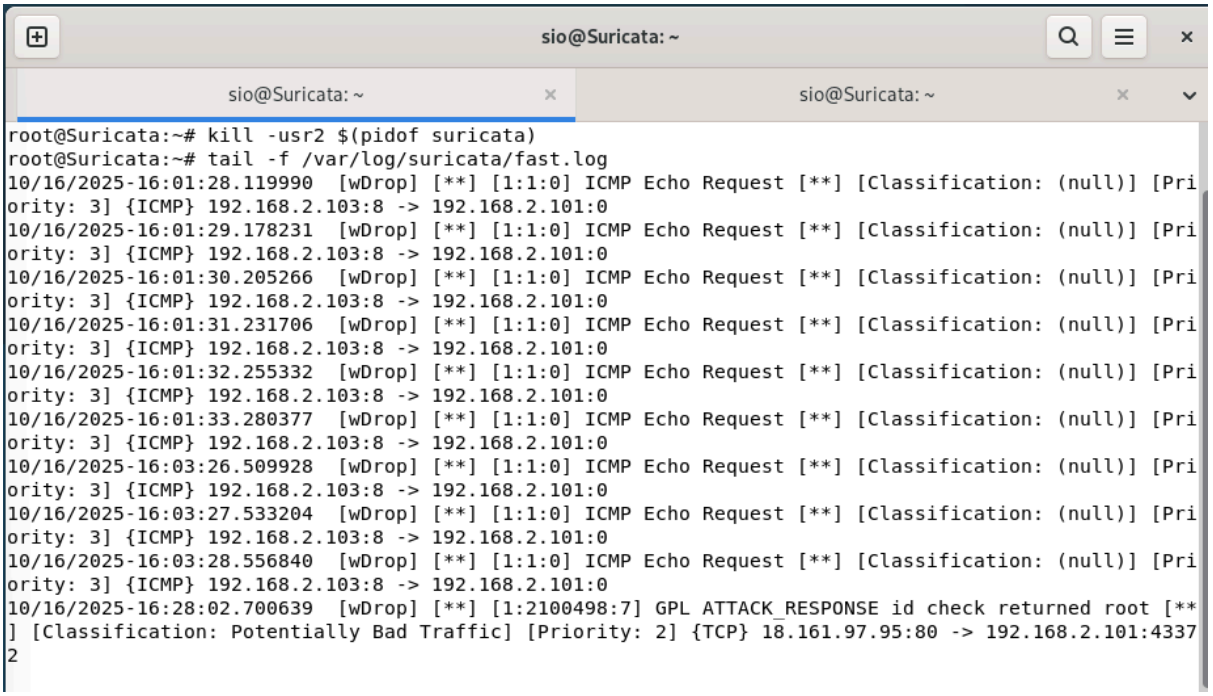


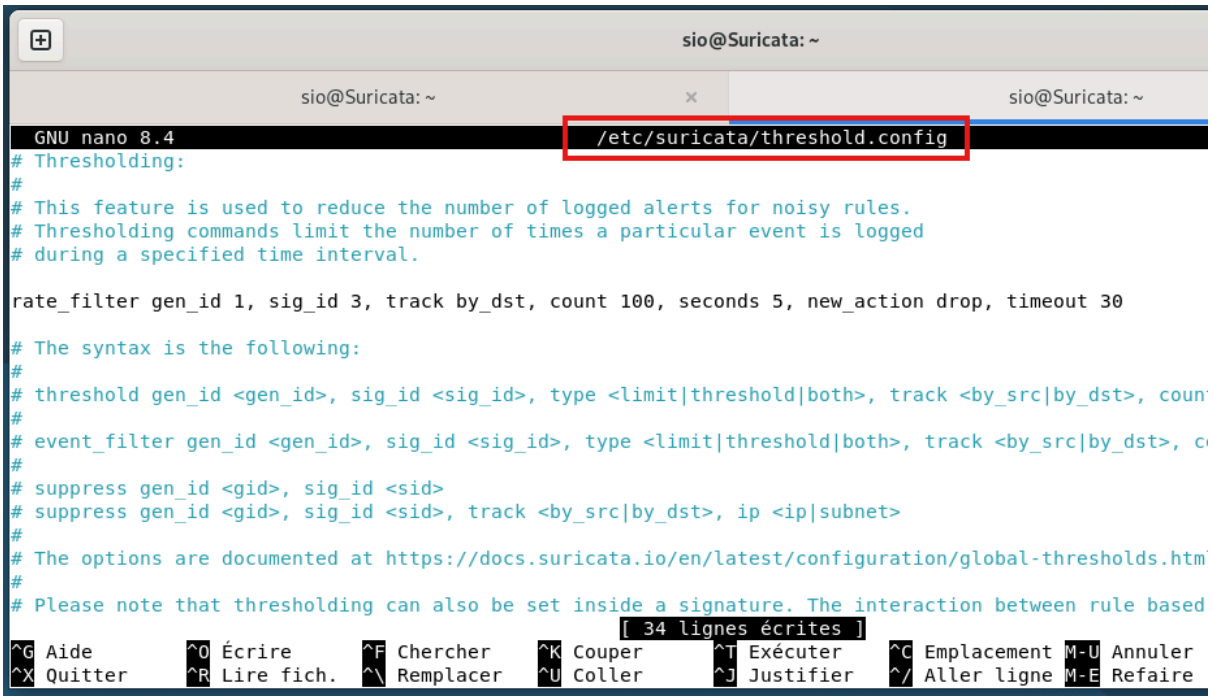

▪ Test avec la commande curl :

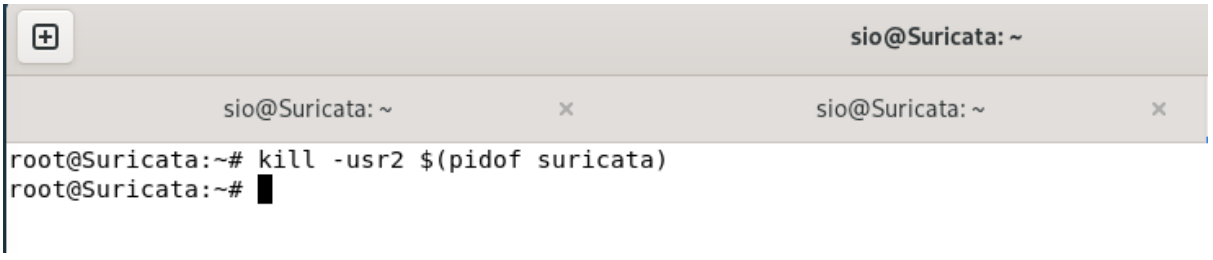


▪ Vérification de l'action Drop dans le log fast.log :

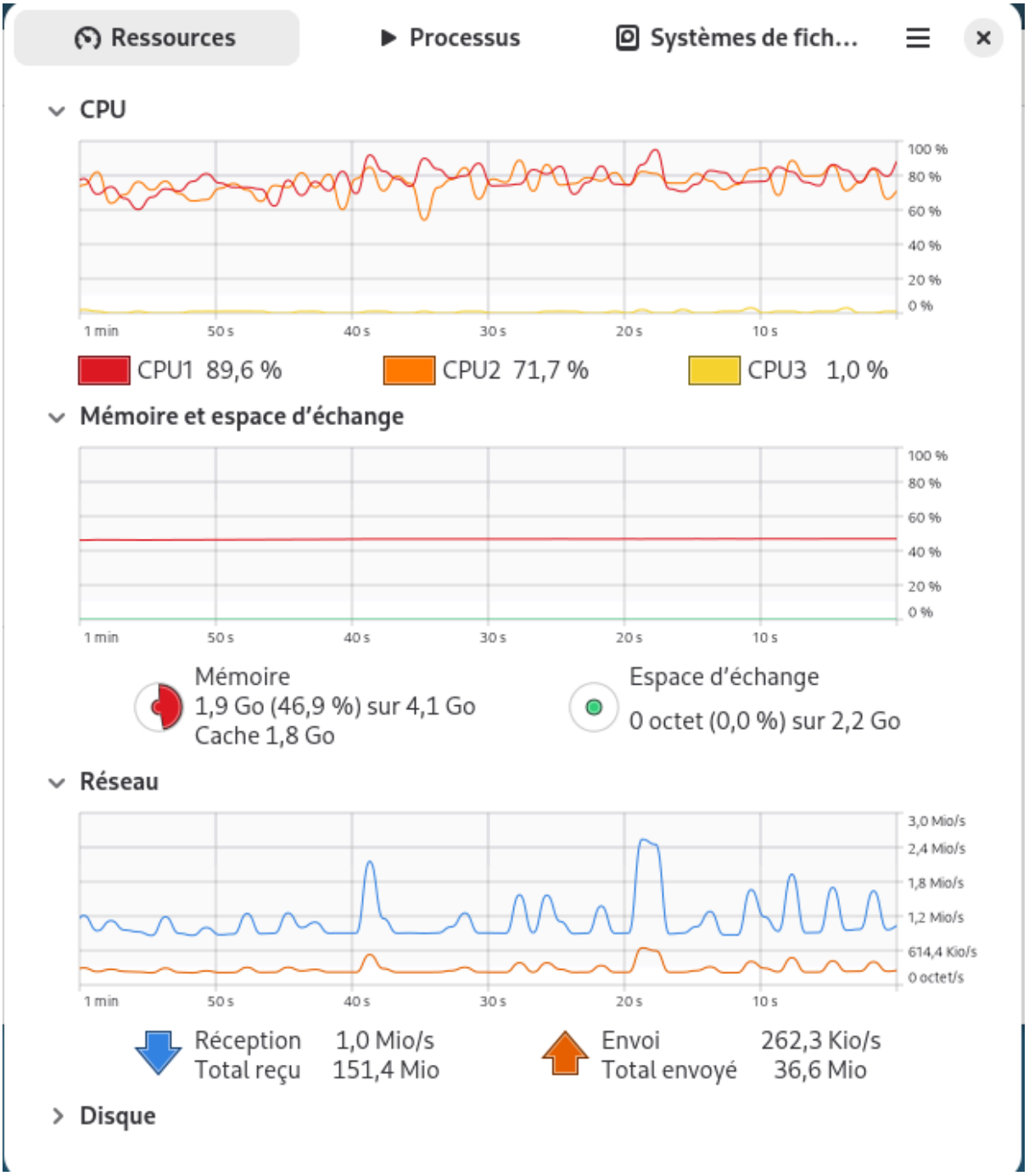


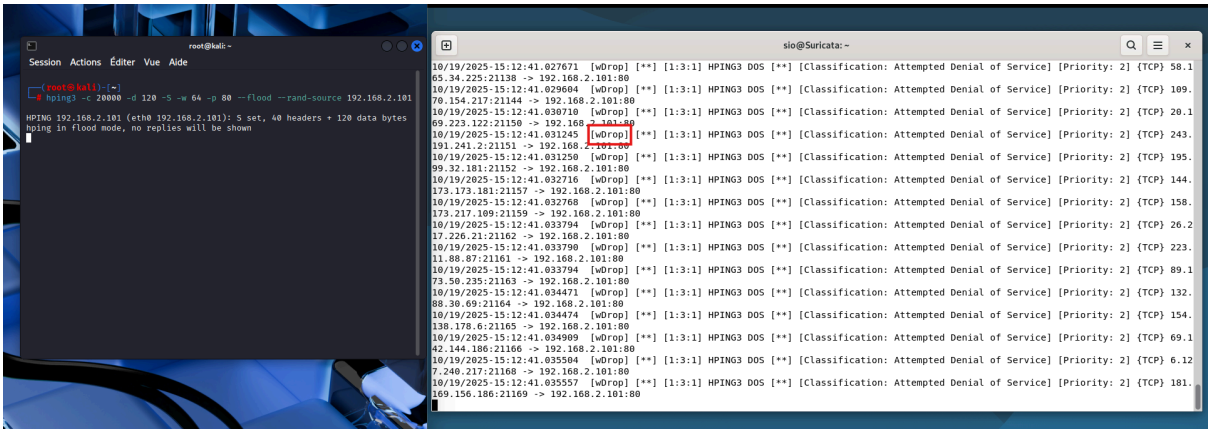
# 9) Créer une règle permettant de bloquer une attaque DOS (SYN Flood) sans bloquer les requêtes http légitimes :

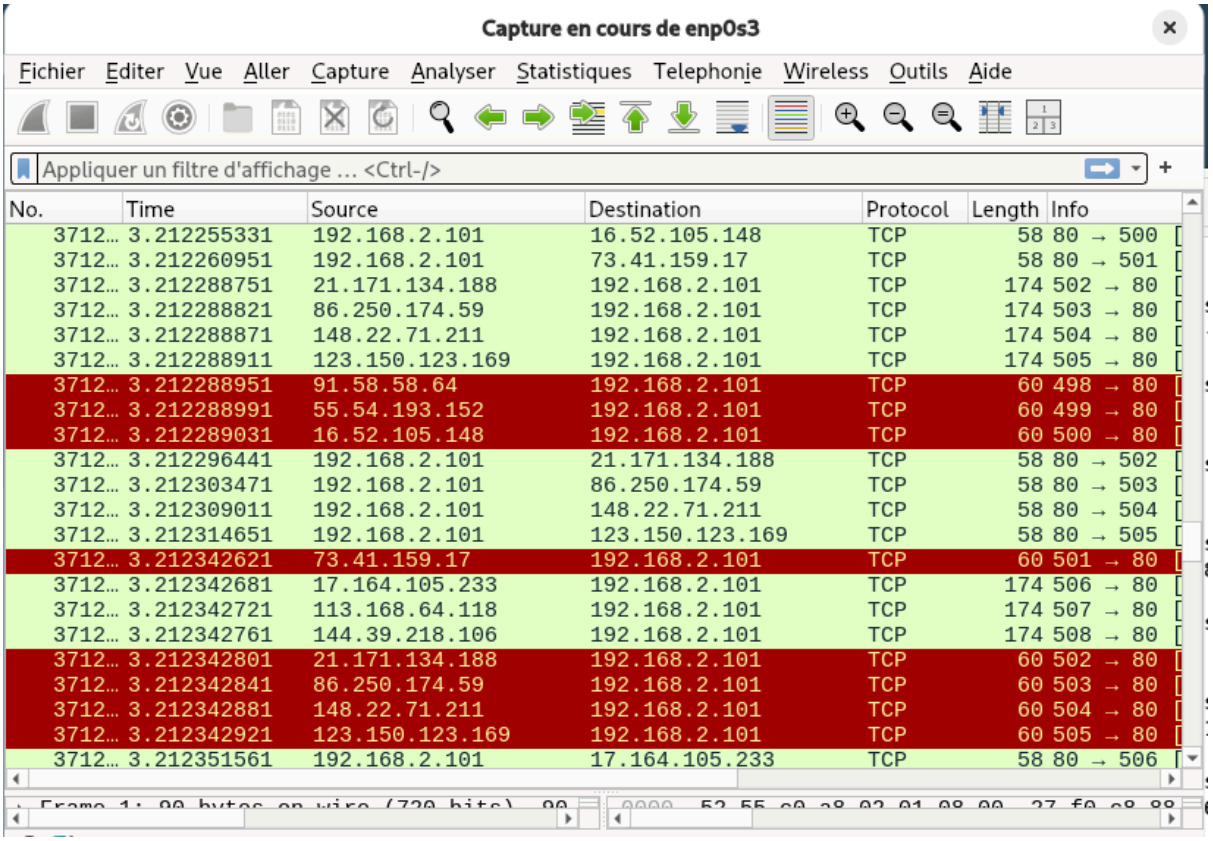



▪ Nous démarrons une capture de trames sur la machine Suricata puis démarrer l'attaque DOS SYN Flood avec hping3 et nous vérifions la suppression des paquets ainsi que la disponibilité de la machine Suricata :
Nous vérifions également avec l'application Moniteur système l'utilisation des ressources CPU/RAM de la machine Suricata.




root@kali: ~
Session Actions Éditer Vue Aide
(root㉿kali)-[~]
# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.2.101
HPING 192.168.2.101 (eth0 192.168.2.101): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
sio@Suricata: ~
10/19/2025-15:12:41.027671 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 58.1
65.34.225:21138 -> 192.168.2.101:80
10/19/2025-15:12:41.029604 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 109.
70.154.217:21144 -> 192.168.2.101:80
10/19/2025-15:12:41.030710 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 20.1
69.223.122:21150 -> 192.168.2.101:80
10/19/2025-15:12:41.031245 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 243.
191.241.2:21151 -> 192.168.2.101:80
10/19/2025-15:12:41.031250 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 195.
99.32.181:21152 -> 192.168.2.101:80
10/19/2025-15:12:41.032716 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 144.
173.173.181:21157 -> 192.168.2.101:80
10/19/2025-15:12:41.032768 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 158.
173.217.109:21159 -> 192.168.2.101:80
10/19/2025-15:12:41.033794 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 26.2
17.226.21:21162 -> 192.168.2.101:80
10/19/2025-15:12:41.033790 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 223.
11.88.87:21161 -> 192.168.2.101:80
10/19/2025-15:12:41.033794 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 89.1
73.50.235:21163 -> 192.168.2.101:80
10/19/2025-15:12:41.034471 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 132.
88.30.69:21164 -> 192.168.2.101:80
10/19/2025-15:12:41.034474 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 154.
138.178.6:21165 -> 192.168.2.101:80
10/19/2025-15:12:41.034909 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 69.1
42.144.186:21166 -> 192.168.2.101:80
10/19/2025-15:12:41.035504 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 6.12
7.240.217:21168 -> 192.168.2.101:80
10/19/2025-15:12:41.035557 [wDrop] [**] [1:3:1] HPING3 DOS [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 181.
169.156.186:21169 -> 192.168.2.101:80


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