TP: Snort 3 - Initial configuration

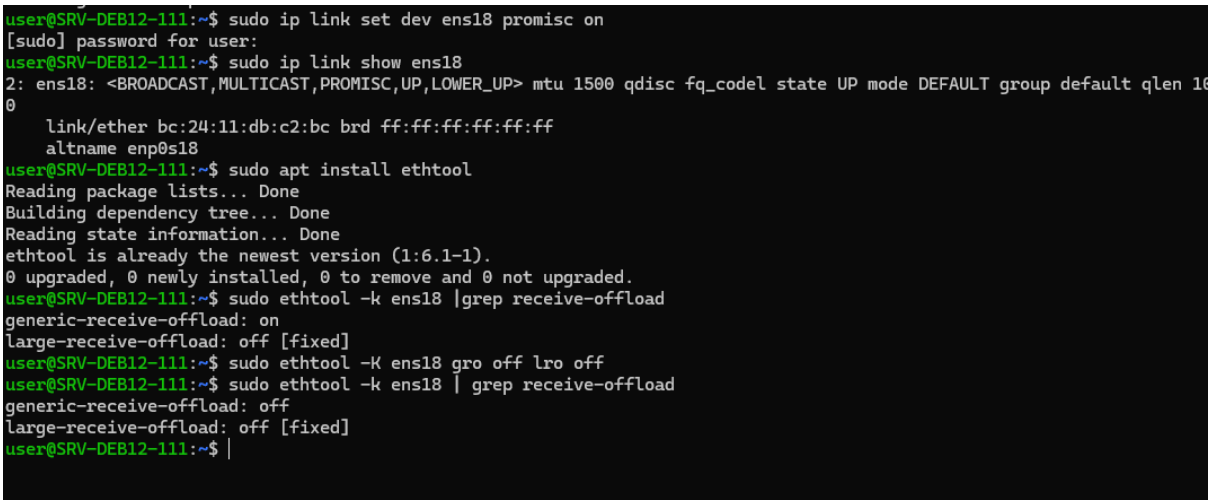
I - CONFIGURATION DE LA CARTE RÉSEAU

1.Activation du mode promiscuous

sudo ip link set dev ens18 promisc on

2.Configuration de l'offload

sudo ip link show ens18
sudo apt install ethtool
sudo ethtool -k ens18 | grep receive-offload
sudo ethtool -K ens18 gro off lro off
sudo ethtool -k ens18 | grep receive-offload



II - CONFIGURATION DU PARAMÉTRAGE AUTO DE LA NIC EN TANT QUE SERVICE

1.Création du fichier de service

sudo nano /etc/systemd/system/snort3-nic.service

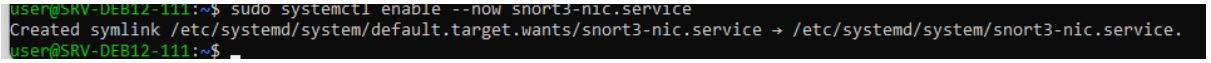
2.Contenu du fichier

[Unit]
Description=Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
After=network.target

[Service]
Type=oneshot
ExecStart=/usr/sbin/ip link set dev ens18 promisc on
ExecStart=/usr/sbin/ethtool -K ens18 gro off lro off
TimeoutStartSec=0
RemainAfterExit=yes

[Install]
WantedBy=default.target

3.Activation et redémarrage du service
systemctl daemon-reload
systemctl start snort3-nic.service
systemctl enable --now snort3-nic.service



III - CREATION D'UN FICHIER DE RÈGLES PERSONNALISÉES

1.Création du répertoire de règles
mkdir /etc/snort/rules

2.Création du fichier de règles
nano /etc/snort/rules/local.rules

3.Contenu du fichier

LOCAL RULES

This file intentionally does nots come with signatures. Put your local additions here.

alert icmp any any -> any any (msg:"!!! ICMP Alert !!!";sid:1000001;rev:1;classtype:icmpevent;)

IV - CONFIGURATION DES LOGS

1.Création du répertoire
mkdir /var/log/snort
chmod 777 /var/log/snort

2.Modification du fichier de configuration de Snort
nano /etc/snort/snort.lua

3.Modifier le fichier
Se rendre tout en bas du fichier, dans la catégorie "7. configure outputs"

```
--------------------------------------------------------------------------
-- 7. configure outputs
--------------------------------------------------------------------------

alert_fast =
{
    file = true,
    limit = 100000
```

```
}

alert_full =
{
   file = true,
   limit = 100000
}
```

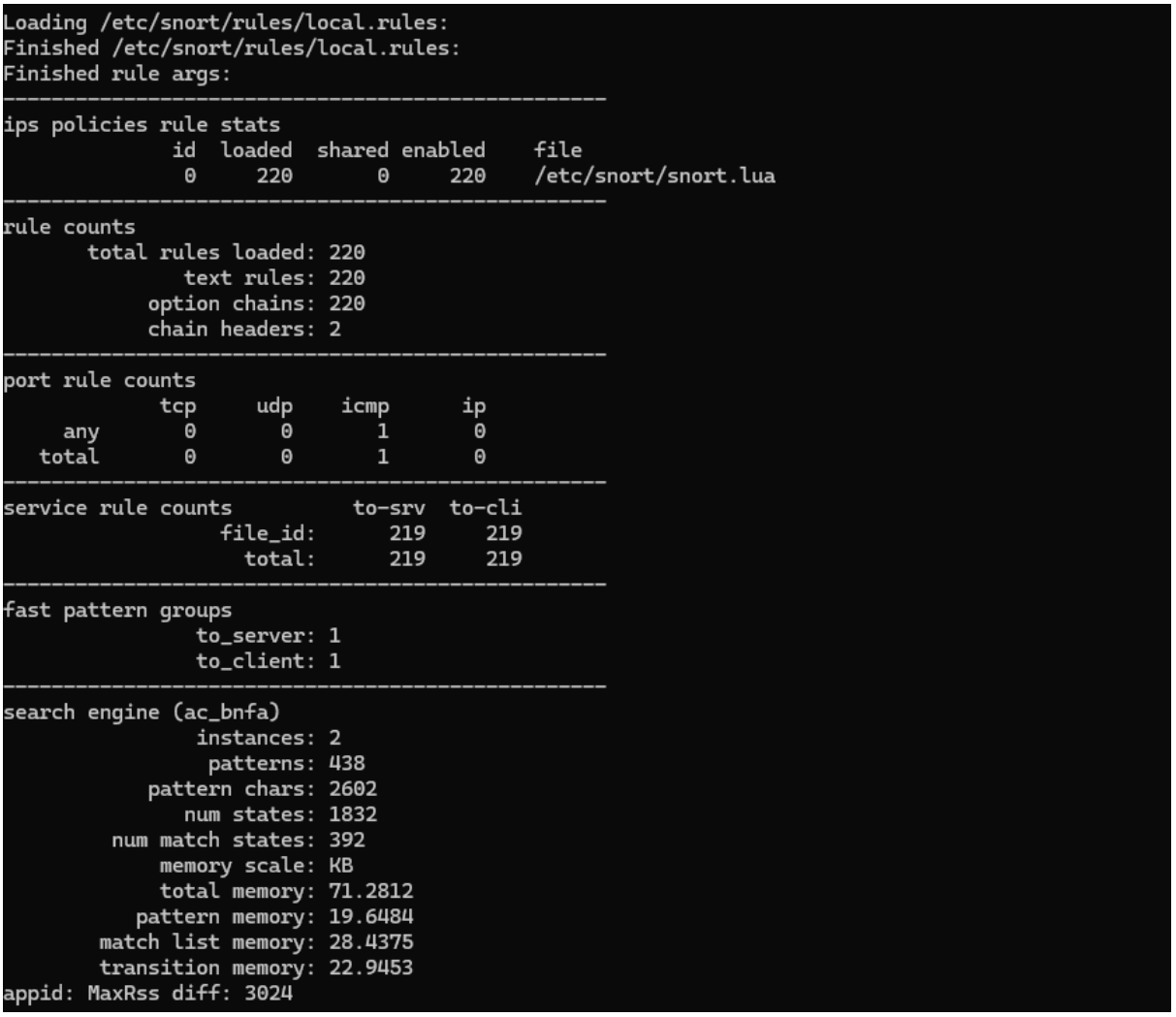
V - TEST

1.Lancer un ping à destination de votre machine

ping 10.0.0.108

2.Lancer la capture Snort

snort -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules -i ens18 -A alert_fast -l /var/log/snort



```
09/30-14:12:49.375999 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:50.377072 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:50.377181 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:51.382790 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:51.382902 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:12:59.465413 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:12:59.465493 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:00.470710 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:00.470819 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:01.494738 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:01.494850 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:02.518727 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:02.518834 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:03.542746 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:03.542856 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:04.566713 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:04.566815 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:05.590876 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:05.590986 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:06.592078 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:06.592194 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:07.593367 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:07.593504 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:08.594632 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:08.594728 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
09/30-14:13:09.622867 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.108 -> 10.0.0.111
09/30-14:13:09.622986 [**] [1:1000001:1] "!!! ICMP Alert !!!" [**] [Priority: 0] {ICMP} 10.0.0.111 -> 10.0.0.108
user@SRV-DEB12-111:~$ ping 10.0.0.108
PING 10.0.0.108 (10.0.0.108) 56(84) bytes of data.
64 bytes from 10.0.0.108: icmp_seq=1 ttl=64 time=0.600 ms
64 bytes from 10.0.0.108: icmp_seq=2 ttl=64 time=0.769 ms
64 bytes from 10.0.0.108: icmp_seq=3 ttl=64 time=0.753 ms
64 bytes from 10.0.0.108: icmp_seq=4 ttl=64 time=0.730 ms
64 bytes from 10.0.0.108: icmp_seq=5 ttl=64 time=0.756 ms
64 bytes from 10.0.0.108: icmp_seq=6 ttl=64 time=0.739 ms
64 bytes from 10.0.0.108: icmp_seq=7 ttl=64 time=0.687 ms
64 bytes from 10.0.0.108: icmp_seq=8 ttl=64 time=0.778 ms
64 bytes from 10.0.0.108: icmp_seq=9 ttl=64 time=0.806 ms
64 bytes from 10.0.0.108: icmp_seq=10 ttl=64 time=0.746 ms
64 bytes from 10.0.0.108: icmp_seq=11 ttl=64 time=0.751 ms
64 bytes from 10.0.0.108: icmp_seq=12 ttl=64 time=0.819 ms
64 bytes from 10.0.0.108: icmp_seq=13 ttl=64 time=0.792 ms
64 bytes from 10.0.0.108: icmp_seq=14 ttl=64 time=0.707 ms
```