SNORT

- **Installation :**
    - apt-get update
    - apt-get install snort
- **Vérification :**
    - snort -v
- **Démarrer Snort :**
    - snort -i enp0s3 -c /etc/snort/snort.conf -A console
        - -i: pour indiquer le nom de interface reseau à utiliser pour écouter le trafic
        - -A: Indique à Snort d' Envoyer des alertes "Fast-style" vers la console
- **Tester le fonctionnement pour le protocole ICMP** :

Ajouter une règle dans /etc/snort/rules/local.rules qui permet de lever une alerte dès la détection d'un paquet qui contient des données ICMP

- Il possible d'enregistrer les paquets dans des fichiers en mode texte en utilisant l'option -l :

  snort -i enp0s3 -c /etc/snort/snort.conf -l /home/ak/Bureau/Mes_log -K ascii