TP 6 : Snort NIDS

1. Préparation du système & installation des dépendances requises

1. Tout d'abord, connectez-vous à l'utilisateur root et mettez à jour votre système en tapant les commandes :

   apt-get update

   apt-get upgrade

2. Installation de Snort

1. Utilisez sudo apt-get install snort.

En cas de problème avec dpkg, tapez la commande : sudo dpkg - - configure –a et faites l'update de logiciels : sudo apt-get upgrade

2. Vérifiez l'installation et la configuration avec la commande :

   snort –V. vous devez voir la version de snort installé

3. **Configuration de snort**

Nous allons configurer Snort pour le mode IDS réseau.

Ouvrez le fichier /etc/snort/snort.conf en tant qu'admin. Apportez les modifications suivantes (remplacez 192.168.15.0/24 votre plage réseau):

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.15.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH  /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include $RULE_PATH/local.rules
```

1. Sauvegarder le fichier de configuration et fermez le.

2. Validez la configuration avec la commande (remplacez eth0 par votre interface réseau):

   snort -T -i eth0 -c /etc/snort/snort.conf

   Si tout est OK, vous devez avoir le message suivant affiché :

   Snort successfully validated the configuration!

   Snort exiting

4. **Test snort**
   1. Editez le fichier /etc/snort/rules/local.rules
   2. Ajoutez les lignes suivantes :

      alert tcp any any -> $HOME_NET 21 (msg:"FTP connection attempt"; sid:1000001; rev:1;)

      alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)

      alert tcp any any -> $HOME_NET 80 (msg:"TELNET connection attempt"; sid:1000003; rev:1;)
   3. Sauvegardez et fermez le fichier
   4. Démarrer Snort en mode NIDS (on suppose que eth0 est votre interface réseau):

      snort -A console -q -c /etc/snort/snort.conf -i eth0

      maintenant snort en écoute de l'interface eth0
   5. Faites des essais de ping, ftp et telnet depuis une autre machine :

      ping 192.168.15.189

      ftp 192.168.15.189

      telnet 192.168.15.189 80

      En supposant que 192.168.15.189 est l'adresse IP du serveur snort.