Sadek

Adel

Mise en place d'une sonde sorte

La sonde snort va permettre de « sniffer » tout le trafic qui passe par la machine et donc de lancer certaines alerte lorsque qu'il y'a certain paquet avec des protocoles de transport spécifique (TCP, UDP) ou des protocoles qui relève du niveau 7 application (pop,ssh,dns).

Je vais suivre ce tuto

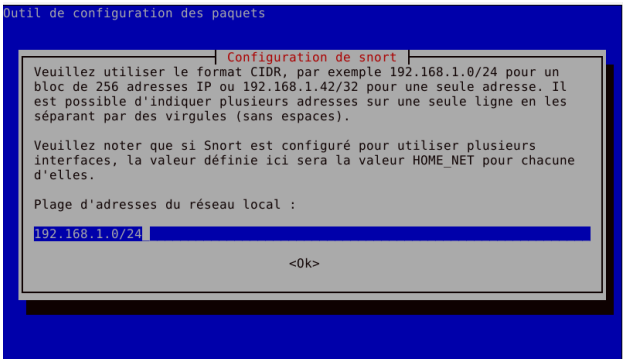
https://all-it-network.com/snort/

https://jacquesgoueth.blogspot.com/2017/07/comment-mettre-en-place-un-systeme-de.html

Snort est un IDS il permet de détecter le trafic malveillant mais ne fait aucune action pour le bloquer contrairement à un IPS

-J'installe le paquet snort

Ensuite cette page s'affiche me demandant l'adresse réseau de mon LAN avec le masque en CIDR

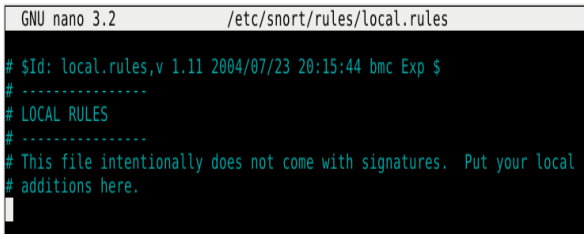


Je valide et l'installation poursuit.

Le fichier pour définir les règles est le

/etc/snort/rules/local.rules

Le fichier à la base ressemble à sa



Ensuite je rajoute cette règle pour recenser tous les pings à destination d'une ip de mon réseau qui passe par ma machine plus précisément sur l'interface eth0 qui est celle choisit par défaut.

alert icmp any any -> $HOME_NET any (msg:"Tentative connexion ICMP"; sid:00001; rev:1;)

Alert = générer une alerte.

ICMP = Le protocole surveiller

Any = la première source la seconde destination

$HOME_NET = Variable que l'on a défini tout à l'heure c'est l'ip de mon réseau (ce qui va vers les ip de mon réseau)

Msg = Le message qui apparaitra

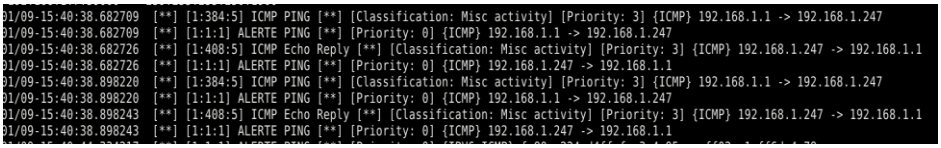
Sid = Numéro unique qui identifie la règle

Rev = Je ne sais pas.

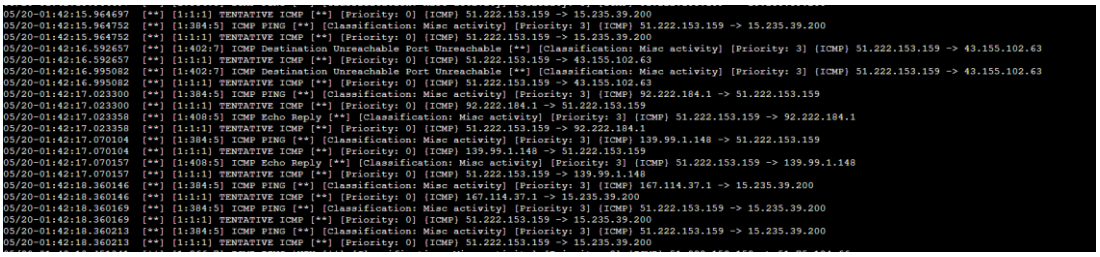
Je lance snort comme ceci

Snort -A console -i eth0 -u snort -c /etc/snort/snort.conf

Je lance un ping depuis une machine sur le réseau vers la machine qui a snort



#Update le 20/05/2022 un autre screen avec une autre machine



On voit bien une alerte ping la source et la destination l'ip de ma machine(snort) est 192.168.1.247

Pour avoir une panoplie complété de règle par défaut on peut aller sur le site de snort et il y'a un fichier .tar.gz (archive compresser) qui contient plein de règles il est à cette adresse

Je regarde ma version de snort (2.9) et je télécharge le fichier qui correspond

https://snort.org/downloads/#rule-downloads

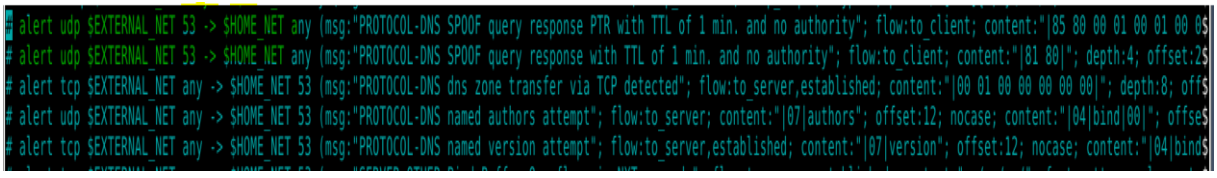
https://snort.org/downloads/community/community-rules.tar.gz

Je le télécharge via wget ensuite je vais dans le dossier décompresser et le déplace le fichier community.rules dans ce répertoire

/etc/snort/rules

Ensuite je me rends dans ce fichier avec nano on voit que la majorité est commenté

Par exemple ici une règle spéciale pour le DNS on voit que c'est du UDP et qui vient du port 53 donc c'est pour prévenir du DNS spoof



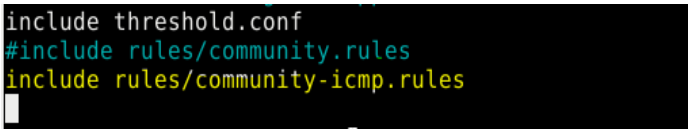
Ensuite je vais dans le fichier /etc/snort/snort.conf et je rajoute la prise en compte de mon nouveau fichier de règles comme ceci

include $RULE_PATH/community.rules

Bon ça n'a pas l'air de marcher sa m'affiche une erreur bitmask unknown je verrai sa plus tard.

Je vais me contenter des règles par défaut qui sont dans le fichier /etc/snort/rules

Je vais rajouter cette règle



Pour lire les fichiers il faut utiliser tcpdump -r (pour lecture)

Car c'est le même format que les fichiers .cap

Ou sinon snort -r /fichier/log

Ne pas oublier de faire dpkg-reconfigure snort pour notamment préciser son mail pour l'envoie des log etc

Snort -A console -l /var/log/snort/ -u snort -c /etc/snort/snort.conf

Pour rediriger les résultats vers un fichier de log visible on peut simplement faire une redirection vers un fichier

snort -A console -c snort.conf > /var/log/snort/log.test.log

Pour envoyer les alertes dans un fichier et qu'elle ne soit plus qu'afficher dans les logs il faut faire ceci

snort -A full -c /etc/snort/snort.conf

Les alertes seront envoyées dans le fichier /var/log/snort/alert

Voici un extrait

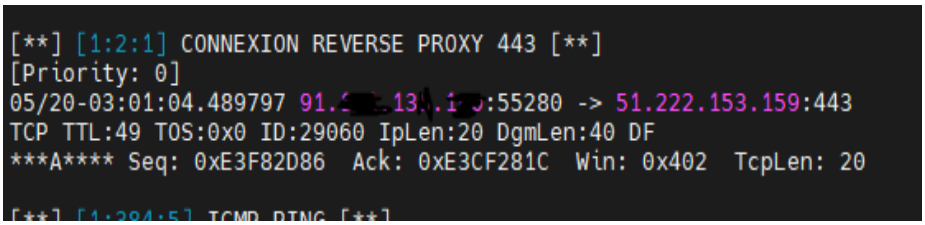
```
[**] [1:1:1] TENTATIVE ICMP [**]
[Priority: 0]
05/20-02:49:16.788690 51.222.153.159 -> 92.222.186.1
ICMP TTL:64 TOS:0x8 ID:2818 IpLen:20 DgmLen:32
Type:0  Code:0  ID:49830  Seq:1  ECHO REPLY
```

Petite précision sur les règles snort

Après l'ip source ou destination on peut mettre le port

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
alert tcp $EXTERNAL_NET any -> $HOME_NET 21
```

Ici par exemple j'ai fait une règle qui me permet de loguer les paquets vers mon reverse proxy

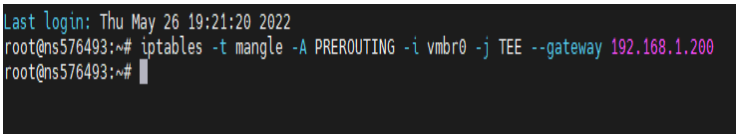


Port mirroring avec iptables

La prochaine étape sera de rajouter une machine dans le contexte ou sera héberger SNORT et une copie des paquets lui sera envoyer avec iptables avec cette commande

iptables -t mangle -A PREROUTING -i eth0 -j TEE --gateway <IP_machine_clone>

Ce qui me permettra d'isoler mon IDS et de ne pas charger les logs de mon serveur et de vraiment appliquer la philosophie d'un IDS qui est un équipement qui reçoit l'ensemble du trafic pour ensuite l'analyser.

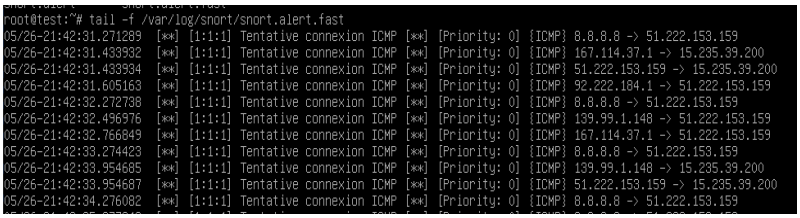


Mangle = Le rôle principal de cette table devrait être de modifier des paquets.

Du coter de l'IDS sur la nouvelle je le lance comme montrer plus haut.

Je scan le trafic qui vient de l'extérieur de mon réseau avant de rentrer à l'intérieur du réseau si j'aurai voulu scanner le trafic après qu'il soit filtré j'aurais posé scanner le trafic sortant de l'interface qui est dans mon LAN et non dans mon WAN

Résultat =



Cela fonctionne parfaitement.

Jusqu'à maintenant on a mis en place un IDS baser sur la politique de la confidentialité.

On peut combiner plusieurs méthodes avec snort en important des règles etc.

Envoyer les logs vers un serveur rsyslog

Il faut d'abord envoyer les logs snort vers un « local » ce « local » permet de rajouter des « cases de surveillance » à rsyslog

Cela ce fait dans le fichier de configuration « snort.conf »

```
output alert_syslog: LOG_LOCAL5 LOG_ALERT
```

Ceci c'est pour que toute les alertes soient envoyées

Ensuite dans le fichier rsyslog.conf sur le client

```
local5.*        @192.168.1.137
*.*     @192.168.1.137
```

Le résultat sur le serveur :