



SECURINETS
Club de la sécurité informatique
INSAT

Atelier : Intrusion Prevention System IPS -SNORT INLINE

**Securinetsiens : 1. Rayan Ktari
2. Sameh Ben Ahmed
3. Henda Boussaid
4. Hassan Jemmali
5. Aymen Bouchriha**

1. Présentation :

Un IDS (Intrusion Detection System) journalise une alerte quand un paquet correspond à une règle de signature mais ne le rejette ou même ne le modifie pas. Ceci est différent avec un IPS (Intrusion Prevention System) où un paquet correspondant à une règle de signature est bloqué ou modifié.

Il faut être très attentif avec les "faux positifs" (paquets correspondant à une règle de signature mais étant en fait inoffensifs) sur un IPS parce que ceci peut nuire au bon fonctionnement des communications entre vos systèmes en bloquant des liens requis pour le business.

Pour nos tests, nous avons utilisés Snort_Inline 2.4.5a et Ubuntu LTS 6.06 (dapper). Nous avons remarqué des problèmes lors de l'utilisation de Fedora et Redhat et d'Ubuntu 6.10 (edgy) ou snort_inline-2.6.1.2-B1.

2. Outils et installations :

- APACHE2 - serveur web.
Version installée sur notre Linux: 2.0.55
- MySQL - base de données.
Version installée: 5.0.22
- PHP5 - langage de script orienté serveur.
Version installée: 5.1.2
- PHP5-MySQL
Version installée: 5.1.2
- BUILD-ESSENTIAL - metapackage contenant des outils pour compiler et installer des programmes. Version installée: 11.1



SECURINETS

Club de la sécurité informatique
INSAT

- PCRE 🌐 - librairie de fonctions utilisant la même syntaxe et sémantique que Perl 5.
Version installée: 6.4.1
- IPTABLES-DEV 🌐 - Set de règles de filtrage pour Linux.
Version installée: 1.3.3
- LIBNET 🌐 - interface de programmation générique réseau qui fournit un accès à plusieurs protocoles.
Version installée: 1.0.2a-7

Soyez attentif à **ne pas installer libnet 1.1.x** (package libnet1-dev). Sinon, comme indiqué sur le [site web de Snort Inline](#), la compilation de Snort_Inline contre cette version de libnet ne fonctionnera pas.

■ LIBRAIRIE MYSQLCLIENT - librairies de développement MySQL et fichiers "header". Version installée: 4.0.24

■ LIBDNET 🌐 - interfacage vers des routines réseaux de bas niveau.
Version installée: 1.11

SNORT INLINE :

Il est obligatoire d'avoir les outils pré requis pour pouvoir compiler Snort_Inline avec succès..

```
#tar -xvf snort_inline-2.4.5a.tar.gz
```

Créez deux dossiers, un pour stocker le fichier de configuration, l'autre pour stocker les règles Snort.

```
#mkdir /etc/snort_inline  
#mkdir /etc/snort_inline/rules
```

Copiez les fichiers de configurations de Snort_Inline dans le dossier /etc/snort_inline/.

```
#cp snort_inline-2.4.5a/etc/* /etc/snort_inline/
```

A l'intérieur du fichier /etc/snort_inline/snort_inline.conf, recherchez la ligne commençant par "var RULE_PATH" et changez la comme ci-dessous:

```
var RULE_PATH /etc/snort_inline/rules
```



SECURINETS

Club de la sécurité informatique
INSAT

Copiez deux fichiers à l'intérieur de notre nouveau dossier `/etc/snort_inline/rules`:
- `classification.config`: définit des URLs pour les références trouvées dans les règles.
- `reference.config`: inclut de l'information pour la priorité des règles.

```
#cp snort_inline-2.4.5a/etc/classification.config /etc/snort_inline/rules/  
#cp snort_inline-2.4.5a/etc/reference.config /etc/snort_inline/rules/
```

Créez un dossier de journalisation:

```
#mkdir /var/log/snort_inline
```

3-COMPILATION ET INSTALLATION DE SNORT

```
#cd snort_inline-2.4.5a  
#./configure --with-mysql
```

Si vous avez installés toutes les dépendances correctement, la commande "configure" doit se terminer sans la moindre erreur!

Si par malheur, vous avez un message d'erreur, référez-vous au bas de la page.

Compilons et installons snort_Inline.

```
#make  
#make install  
Netfilter & Snort_Inline
```

NetFilter est un module du noyau de Linux disponible depuis la version 2.4 du noyau. Il fournit trois principales fonctionnalités:

- filtrage de paquet - Accepte ou rejette des paquets
- NAT - Change la source ou la destination IP d'un paquet réseau
- "Packet Mangling" - Modifie les paquets (utilisé par exemple pour la qualité de service, QoS)

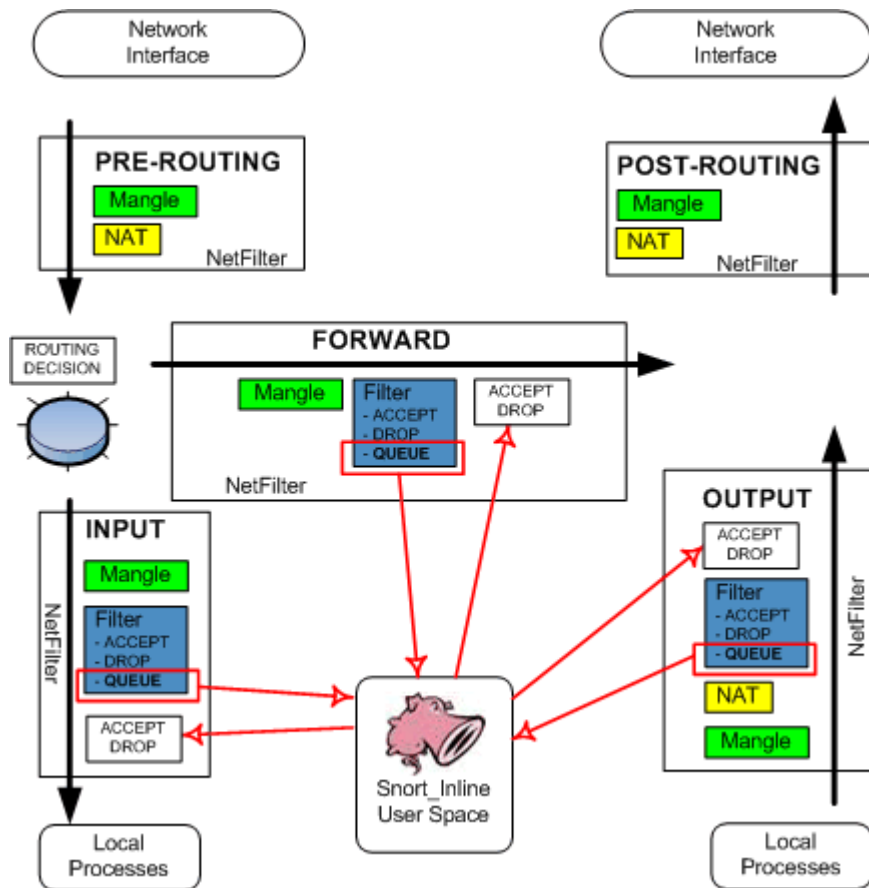
Iptables est un outil pour configurer Netfilter. Il doit être lancé en tant que root.

Netfilter met en queue des paquets vers Snort_Inline dans l'espace utilisateur (user space) avec l'aide du module du noyau Linux `ip_queue` et `libipq`.

Puis, si un paquet correspond à une signature d'attaque de Snort_Inline, il est marqué par `libipq` et revient vers le noyau où est rejeté.



SECURINETS
Club de la sécurité informatique
INSAT



Deux modes Snort_Inline sont disponibles:

→ "Drop Mode" (mode rejet)

Les paquets sont rejetés si ils correspondent à une signature d'attaque, ce mode est celui que nous utilisons dans notre tutorial

Trois options sont disponibles dans ce mode:

- Drop: rejette un paquet, envoie un message "reset" vers l'émetteur, journalise l'événement.
- Sdrop: rejette un paquet sans envoyer un message "reset" en retour vers l'émetteur.
- Ignore: rejette un paquet, envoie un message "reset" vers l'émetteur, ne journalise pas l'événement.

→ "Replace Mode" (mode remplacement)

The packets are modified if they match an attack signatures.

Nous devons charger le module ip_queue et vérifier si l'opération a bien été effectuée:

```
#modprobe ip_queue  
#lsmod | grep ip_queue
```



SECURINETS
Club de la sécurité informatique
INSAT

Pour télécharger ip_queue:"modprobe -r ip_queue"

Configuration d'Iptables pour tester Snort_Inline

Il s'agit maintenant d'effectuer des tests pour voir si tout marche bien.
Tout d'abord nous avons besoin de configurer Netfilter avec l'outil Iptables.
Nous configurons ci-dessous une règle Netfilter pour envoyer tout le trafic entrant vers la queue où il sera analysé contre les règles de Snort_Inline.

iptables -A INPUT -j QUEUE

Vérifiez vos règles:

#iptables -L

Si vous voulez supprimer vos règles Iptables: "iptables -F"

Lancement de Snort_inline

#snort_inline -Q -v -c /etc/snort_inline/snort_inline.conf -l /var/log/snort_inline

-Q -> process le trafic mis en queue
-v -> verbose
-l -> chemin des journaux (logs)
-c -> chemin du fichier de configuration

4-Test :

1. Premier test

Nous pouvons simuler une attaque en accédant simplement à une page web située sur la machine Snort_Inline depuis cette même machine parce que ceci correspondra à une règle d'attaque Snort.

Par exemple, vous pouvez ouvrir Firefox et entrer <http://localhost>.

→ Journal rapide (quick log)

#tail -f /var/log/snort_inline/snort_inline-fast

```
03/07-12:39:27.127882 [**] [116:151:1] (snort decoder)  
Bad Traffic Same Src/Dst IP [**] {TCP} 127.0.0.1:41050 -> 127.0.0.1:80
```

```
03/07-12:39:27.127882 [**] [116:150:1] (snort decoder)  
Bad Traffic Loopback IP [**] {TCP} 127.0.0.1:41050 -> 127.0.0.1:80
```

→ Journal complet (full log)



SECURINETS

Club de la sécurité informatique
INSAT

#tail -f /var/log/snort_inline/snort_inline-full

```
[**] [116:151:1] (snort decoder) Bad Traffic Same Src/Dst IP [**]  
03/07-12:37:03.036694 127.0.0.1:53110 -> 127.0.0.1:80  
TCP TTL:64 TOS:0x0 ID:16812 IpLen:20 DgmLen:60 DF  
*****S* Seq: 0x9B74D9F2 Ack: 0x0 Win: 0x7FFF TcpLen: 40  
TCP Options (5) => MSS: 16396 SackOK TS: 115788 0 NOP WS: 2  
[**] [116:150:1] (snort decoder) Bad Traffic Loopback IP [**]  
03/07-12:37:03.036694 127.0.0.1:53110 -> 127.0.0.1:80  
TCP TTL:64 TOS:0x0 ID:16812 IpLen:20 DgmLen:60 DF  
*****S* Seq: 0x9B74D9F2 Ack: 0x0 Win: 0x7FFF TcpLen: 40  
TCP Options (5) => MSS: 16396 SackOK TS: 115788 0 NOP WS:
```

2. Deuxième test

Nous ajoutons une règle de signature pour rejeter tout le trafic web entrant:
Ajoutez la règle suivante dans le fichier /etc/snort_inline/rules/web-attacks.rules.

#vi /etc/snort_inline/rules/web-attacks.rules

```
drop tcp any any -> any 80 (classtype:attempted-user; msg:"Snort_Inline bloque le  
traffic!");
```

→Quick log

#tail -f /var/log/snort_inline/snort_inline-fast

```
04/01-18:11:39.454787 [**] [1:0:0] Snort_Inline bloque le traffic!  
[**] [Classification: Attempted User Privilege Gain] [Priority: 1]  
{TCP} 192.168.1.3:1626 -> 192.168.1.101:80
```

→Full Log

#tail -f /var/log/snort_inline/snort_inline-full

```
[**] [1:0:0] Snort_Inline bloque le traffic! [**]  
[Classification: Attempted User Privilege Gain] [Priority: 1]  
04/01-18:11:39.454787 192.168.1.3:1626 -> 192.168.1.101:80  
TCP TTL:128 TOS:0x0 ID:47535 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0x612540DD Ack: 0x0 Win: 0xFFFF TcpLen: 28  
TCP Options (4) => MSS: 1460 NOP NOP SackOK
```

Est bien sure la page ne s'affiche pas.