

## 0.1 Système de détection d'intrusion : SNORT

S.N.O.R.T. est un NIDS (Network Intrusion Detection System ou Système de Détection d'Intrusion Réseau en français). Comme ses initiales le suggèrent, un NIDS sert à détecter les tentatives d'intrusion, pour ce faire, il compare le trafic réseau à une base de données des attaques connues. Le cas échéant, il exécute une action prédéfinie, qui va de vous prévenir à verrouiller le réseau. S.N.O.R.T. vous permettra donc basiquement, de détecter d'éventuels intrusions, de gérer vos logs et sniffer le réseau. Nous détaillerons ici, l'installation à partir des sources, bien que de nombreuses distributions soient livrées avec un paquetage snort. Ce choix est motivé par deux choses : d'abord le fait qu'il soit impossible d'étudier toutes les variations introduites par les distributions, mais surtout pour un logiciel aussi sensible, il est préférable d'en maîtriser tous les rouages. Néanmoins, la plus part des principes expliqués ici, sont translatables vers les paquets binaires de votre distribution, moyennant quelques adaptations.

### 0.1.1 1. Pré-requis pour Snort :

- Bison (ou yacc), flex et gcc. Tous ces logiciels sont installés où présents sur vos cdroms.
- libpcap que vous trouverez ICI<sup>1</sup> ! lien mort !
- Et bien-sûr Snort ICI<sup>2</sup>

### 0.1.2 2. Installation de libpcap :

Libpcap est une dépendance nécessaire à snort, qui s'installe comme suite :

```
$ tar -xzf /où_est/libpcap.tar.Z
$ cd libpcap-0.4/
$ ./configure --prefix=/usr
$ make
$ su
Password
# make install
# mkdir /usr/include/pcap
# cp *.h /usr/include/pcap/
# mkdir /usr/include/pcap/net
# cp bpf/net/*.h /usr/include/pcap/net/
# make install-man
```

### 0.1.3 3. Installation de Snort :

L'installation de ce logiciel est des plus classiques, tapez simplement les commandes suivantes dans un terminal, en root :

<sup>1</sup> <ftp://ftp.ee.lbl.gov/libpcap.tar.Z>

<sup>2</sup> <http://www.snort.org>

```
# tar -xzf /où_est/snort-1.9.0.tar.gz
# cd snort-1.9.0/
# ./configure --prefix=/usr --with-libpcap-includes=/usr/include/pcap
--with-libpcap-libraries=/usr/lib
# make
# make install
# mkdir /etc/snort/
# mkdir /etc/snort/rules/
# cp etc/snort.conf /etc/snort/
# cp etc/classification.config /etc/snort/
# cp etc/reference.config /etc/snort/
# cp rules/*.rules /etc/snort/rules/
```

Dans la suite nous utiliserons le répertoire `/var/log/snort/`, il est donc indispensable qu'il existe. Si ce n'est pas le cas chez vous, créez-le par :

```
# mkdir /var/log/snort
# mkdir /var/log/snort/alert
```

A ce stade snort est correctement installé, une protection supplémentaire est d'exécuter snort avec les privilèges de l'utilisateur snort, c'est à dire aucun. Commencez par vérifier que vous avez un utilisateur snort :

```
# cat /etc/passwd | grep snort
```

Si vous n'avez aucun résultat, c'est qu'il n'existe pas, il vous suffit de le créer par :

```
# groupadd snort
# useradd -g snort -d /var/log/snort snort
```

Qu'il existe déjà ou pas, ajustez les droits sur `/var/log/snort` par :

```
# chown -R snort /var/log/snort
# chgrp -R snort /var/log/snort
```

#### **0.1.4 4. Utilisation de Snort :**

Comme précédemment indiqué, S.N.O.R.T. remplit globalement 3 tâches, qui sont ses modes de fonctionnement : Sniffer, Packet Logger et NIDS. Les 2 premiers sont relativement triviaux, le dernier requiert plus d'attention.

#### **0.1.5 4.1 Utilisation de Snort en mode Sniffer :**

Il s'agit d'écouter le réseau, en tapant une ou plusieurs lignes de commandes qui indiqueront à snort le type de résultat à afficher, en voici quelques-unes :

- la commande `verbose` affiche les en-têtes TCP/IP :

```
# snort -v
```

L'interface connectée à Internet est automatiquement détectée et scannée. Est-il utile de préciser qu'il faut de l'activité sur votre réseau pour avoir des résultats ?

- la commande `verbose dump second layer info`, affiche les IP et les en-têtes TCP/UDP/ICMP

```
# snort -vde
```

vous obtenez quelque chose approchant : 01/18-13 :19 :34.435271 0 :50 :FC :25 :4 :4  
 -> 0 :50 :FC :E :34 :E8 type :0x800 len :0x4A 192.168.0.7 :33091  
 -> 213.186.34.126 :80 TCP TTL :64 TOS :0x0 ID :15797 IpLen :20  
 DgmLen :60 DF \*\*\*\*\*S\* Seq : 0xA11A3122 Ack : 0x0 Win : 0x16D0  
 TcpLen : 40 TCP Options (5) => MSS : 1460 SackOK TS : 593047  
 0 NOP WS : 0 Au début vous avez la date et l'heure (18 janvier à 13h19), un peu plus loin vous avez l'adresse IP source et le port d'écoute (192.168.0.7 :33091). Immédiatement suivi de l'adresse IP destinataire et du port concerné (213.186.34.126 :80). TCP indique le protocole utilisé, TTL(Time to live) temps à vivre du paquet, TOS (Type Of Service) le type de service et ID un identifiant aléatoire.

- Une autre commande :

```
# snort -dvi eth0
```

Cette fois il faut indiquer l'interface réseau à scanner, il peut s'agir de eth0, ppp0 ...

### 0.1.6 4.2 Utilisation de Snort en mode packet logger :

Ce mode est en tout point similaire au précédent, à ceci près que les logs ne s'affichent plus à l'écran, mais s'inscrivent directement dans un fichier de log. Le répertoire naturel de log de snort étant /var/log/snort/. La seule modification par rapport à précédemment est le v, remplacé par l, concrètement :

```
# snort -de -l /var/log/snort
```

correspond à snort -vde. En visitant le répertoire /var/log/snort/ vous constaterez l'existence de plusieurs répertoires. Chacun correspondant à une adresse source. Il est possible de faire plus fin, en ne loguant qu'une seule classe d'adresses par exemple :

```
# snort -de -l /var/log/snort -h 192.168.0.0/24
```

ou en enregistrant au format binaire :

```
# snort -l /var/log/snort -b
```

Notez enfin qu'il est possible d'interfacer snort avec une base de données (mysql, postgresql, dbc, oracle).

### 0.1.7 4.3 Utilisation de Snort en nids :

Vous l'aurez compris, le véritable intérêt des nids est encore l'utilisation en mode nids. S.N.O.R.T. utilise pour cela des règles pour détecter les intrusions. Il existe aujourd'hui environ 1500 règles différentes, chacune s'adaptant à un cas particulier. Vous pouvez créer des règles pour observer une activité particulière sur votre réseau : pings, scans, connexions par backdoors, faille dans un script, tentative de prise de contrôle à distance ... Les alertes peuvent être enregistrées dans un fichier particulier ou directement dans le syslog et être rajoutées aux messages système ou encore dans une base de données... Chaque règle se rajoute dans un fichier de configuration prévu à cet effet, vous pouvez soit utiliser celles qui existent déjà, soit en créer de nouvelles. Le fichier de configuration de snort est /etc/snort/snort.conf, les fichiers .rules contenus dans /etc/snort/rules/ sont des fichiers contenant, des règles pour un usage bien particulier. Le nom du fichier est, en général explicite, ainsi, ftp.rules contient des règles spécifiques au ftp et dos.rules s'utilise pour les tentatives de DoS (Denial Of Service ou Denie de Service en français). Commençons par mettre à jour le fichier /etc/snort/snort.conf :

- Mettez à jour la classe d'adresse de votre réseau, comme suite (par défaut c'est any) :

```
var HOME_NET 192.168.0.0/24
```

Ceci suppose que vous ayez un réseau local en 192.168.0.x sinon adaptez. Si vous avez plusieurs réseaux utilisant chacun une classe d'adresse particulière, se sera :

```
var HOME_NET [10.0.0.0/24,192.168.0.0/24]
```

- Vous devez également indiquer votre Serveur de DNS, je mets les informations pour wanadoo (de la forme `var $DNS_SERVERS [DNS1/reseau,DNS2/reseau]`) :

```
var $DNS_SERVERS [193.252.19.3/32,193.252.19.4/32]
```

- Indiquez maintenant le répertoire où sont disposés vos règles, dans notre cas :

```
var RULE_PATH ./rules
```

- Décommentez et ajustez les préprocesseurs qui vous intéressent, en voici 2 indispensables :

```
preprocessor portscan : $HOME_NET 4 3 /var/log/snort/portscan.log
preprocessor http_decode : 80 unicode iis_alt_unicode
double_encode iis_flip_slash full_whitespace
```

- Vous devez maintenant indiquer, quel format d'alerte vous souhaitez. Vous avez le choix entre : syslog (logs système), tcpdump, base de données, xml, binaire, mail (snmp), à l'écran ou dans le fichier de log. Selon le mode choisi, reportez-vous à la documentation associée.

Si vous souhaitez utiliser syslog (`/var/log/messages`), décommentez (enlevez le # devant) la ligne suivante :

```
output alert_syslog : LOG_AUTH LOG_ALERT
```

Si vous souhaitez utiliser le répertoire `/var/log/snort/`, ne décommentez aucune ligne, vous fixerez cela directement au lancement avec comme option :

```
-l /var/log/snort
```

Si vous souhaitez afficher, le tout directement à l'écran, il faudra utiliser l'option verbose (-v).

- Il existe six modes d'alerte disponibles, fixables dynamiquement (au lancement) : full, fast, socket, syslog, smb (winpopup), et none (aucun). Quatre de ces modes sont accessibles avec l'option -A.

Ses quatre options sont :

- **-A fast** : mode d'alerte rapide, affiche l'alerte dans un format simple avec l'horaire, le message d'alerte, les adresses IP et les ports sources et destinations
- **-A full** : c'est aussi le mode d'alerte par défaut, donc si vous ne spécifiez rien ceci sera automatiquement utilisé
- **-A unsock** : envoie les alertes à une socket UNIX qu'un autre programme peut écouter
- **-A none** : arrête les alertes
- Vous devez maintenant inclure les autres fichiers de configuration :

```
include classification.config
include reference.config
```

- Dernière tâche, inclure les fichiers.rules qui vous intéressent. Je vous donne une copie du mien :

```
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
# include $RULE_PATH/telnet.rules
# include $RULE_PATH/rpc.rules
# include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/web-cgi.rules
# include $RULE_PATH/web-coldfusion.rules
# include $RULE_PATH/web-iis.rules
# include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
# include $RULE_PATH/oracle.rules
include $RULE_PATH/mysql.rules
include $RULE_PATH/snmp.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop3.rules
include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/shellcode.rules
include $RULE_PATH/policy.rules
# include $RULE_PATH/porn.rules
include $RULE_PATH/info.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/virus.rules
include $RULE_PATH/chat.rules
```

```
include $RULE_PATH/multimedia.rules
include $RULE_PATH/p2p.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/local.rules
```

Vous avez des mises à jour régulières ici<sup>3</sup>

– Il ne vous reste plus qu'à le lancer :

```
# snort -u snort -g snort -A full -d -D -i eth0 -l /var/log/snort
-c /etc/snort/snort.conf
```

Cette ligne de commande indique que snort est lancé avec les privilèges de l'utilisateur "snort" appartenant au groupe "snort", type d'alerte : full. Snort sera lancé en tant que daemon (-D), il regardera l'interface réseau eth0. Selon votre configuration, vous indiquerez plutôt : ppp0, eth1... Snort utilisera le répertoire /var/log/snort/ et le fichier de configuration /etc/snort/snort.conf. Pour que snort, soit lancé à chaque démarrage, il vous suffit de rajouter la ligne précédente à la fin de votre /etc/init.d/rc.local.

### 0.1.8 5. Conclusion :

Ce document ne constitue qu'une entrée en matière à S.N.O.R.T. consultez la documentation officielle pour plus de détails. Je laisse quelques liens utiles : Le site officiel<sup>4</sup> de snort SnarfSnort<sup>5</sup> (! lien obsolète !) une interface graphique pour snort ACID<sup>6</sup> une autre interface graphique pour snort Sniffer son réseau avec Wireshark et Snort<sup>7</sup> **Interface graphique pour SNORT : AcidBASE!** A propos des interfaces graphiques pour SNORT : il est nécessaire de faire une recherche actualisée en la matière. BASE remplace Acid Je signale les liens suivant concernant Base l'interface pour Snort : Ces différents liens proposent généralement l'installations à partir des sources. J'ai expérimenté que sur Debian, les installations à partir des packets Debian fonctionnaient mal, demandant en fait plusieurs interventions supplémentaires ! SNORT et Base (openManiak)<sup>8</sup> ainsi que : SNORT et Base (gizeek)<sup>9</sup> pour une installation DEBIAN à partir d'apt-get : SNORT et Base (bastien Louche)<sup>10</sup> Les tutoriels suivants détaillent plus précisément les installations de BASE en plus de SNORT : à partir des packages ubuntu : Installation d'un IDS SNORT BASE<sup>11</sup> à partir des sources : Le problème que l'on rencontre actuellement vient du fait que le site officiel de SNORT sépare les sources de snort de celle des règles. Or les fichiers de règles ne sont accessibles que si l'on s'inscrit et c'est PAYANT pour 23 euros environ !!! Donc, il faut en passer par les packages de sa distribution !

<sup>3</sup><http://www.snort.org/downloads/rules/>

<sup>4</sup><http://www.snort.org/>

<sup>5</sup><http://www.silicondefense.com/software/snortsnarf/index.htm>

<sup>6</sup><http://www.andrew.cmu.edu/%7Eerdanyliw/snort/snortacid.html>

<sup>7</sup><http://www.funix.org/fr/linux/ethereal.htm>

<sup>8</sup>[http://openmaniak.com/fr/snort\\_tutorial\\_base.php](http://openmaniak.com/fr/snort_tutorial_base.php)

<sup>9</sup><http://www.gizeek.com/2010/04/18/tutodetection-dintrusion-avec-snort-et-b-a-s-e/>

<sup>10</sup><http://www.bastien-louche.fr/2010/02/installation-snort-base-ids-debian/>

<sup>11</sup>[http://www.cllfst.tuxfamily.org/index.php?option=com\\_content&view=article&id=95:implementation-dun-ids-snort-part-2&catid=40:zoom&Itemid=62](http://www.cllfst.tuxfamily.org/index.php?option=com_content&view=article&id=95:implementation-dun-ids-snort-part-2&catid=40:zoom&Itemid=62)