Installation de l'IDS SNORT

par julien Lecubin

Introduction

Ce document va tenter d'expliquer les différentes étapes pour mettre en place le détecteur d'intrusions SNORT à partir des sources. Un détecteur d'intrusions s'appelle aussi "IDS" pour Intrusion Detection System. SNORT est un système de détection d'intrusions réseau en OpenSource, capable d'effectuer l'analyse du trafic en temps réel. On l'utilise en général pour détecter une variété d'attaques et de scans tels que des débordements de tampons, des scans de ports furtifs, des attaques CGI, des scans SMB, des tentatives d'identification d'OS, et bien plus.

Avant de commencer l'installation de SNORT, vous devez avoir installé :

PACKAGES	REMARQUES
`MySQL`	La base de données MySQL
`MySQL-client`	La partie cliente de mysql (connexion BD)
`php-mysql`	le module php de mysql
`Apache`	Le serveur web Apache
`mod_php`	Le module php pour Apache
`libpcap/libpcap0-devel`	Librairie utilisée par SNORT pour capturer les paquets (rpm téléchargeable sur rpmfind.net)
`gcc`	indispensable pour compiler les sources de SNORT

Si vous n'avez pas encore installé le trio Apache/PHP/MySQL, il y a un article sur Lea vous expliquant comment le faire. C'est ici.

Les étapes pour l'installation de SNORT sont les suivantes :

- Installation de l'outil SNORT
- Installation des règles SNORT
- Liaison Mysql et SNORT
- Mise en place de ACID (Interface php pour visualiser les logs SNORT)

Installation de SNORT

Téléchargez la dernière release de SNORT à l'adresse suivante : http://www.SNORT.org/dl . La compilation de ce programme reste traditionnelle :

COMMANDES	REMARQUES
`cd /usr/local/snort`	...
`tar -xvzf SNORT-1.9.*.tar.gz`	Décompacte l'application
`./configure --with-mysql=/usr/lib/mysql`	Retirez l'argument `--with-mysql` si vous ne souhaitez pas rediriger les logs SNORT vers une base de données mysql *
`make`	Compilation
`make install`	Installation

Pour l'argument `--with-mysql`, vous pouvez l'adapter si vous utilisez une base de données autre que MySQL :

- `--with-odbc=$PATH_ODBC` : pour une base de données Microsoft SQL server
- `--with-postgresql=$PATH_POSTGRE` : pour une base PostegreSQL
- `--with-oracle=$ORACLE_HOME` : pour une base de données Oracle.

Installation des règles SNORT

Maitenant, il faut télécharger les règles de SNORT. En effet, SNORT utilise des règles pour détecter les intrusions. Il existe aujourd'hui environ 1200 règles différentes. Ces règles se caractérisent par un ensemble de fichiers (ftp.rules, p2p.rules,telnet.rules etc...). Vous devez téléchargez les sources de ces règles à l'adresse suivante :
http://www.SNORT.org/dl/signatures

Créez le répertoire de configuration SNORT, et installez-y les règles :

COMMANDES	REMARQUES
`mkdir /etc/snort`	Création du répertoire contenant la configuration SNORT
`cp /usr/local/snort*/etc/snort.conf /etc/snort`	Copie du fichier de config snort dans /etc/snort
`cp snortrules.tar.gz /etc/snort`	Mise en place des règles dans le répertoire de configuration SNORT
`cd /etc/snort`	On se place dans le répertoire de configuration SNORT
`tar -xvzf snortrules.tar.gz`	Décompactage des règles

Les règles SNORT sont alors placées dans le répertoire `/etc/snort/rules`.

Maintenant, Il faut éditer le fichier de configuration snort (`/etc/snort/snort.conf`) et spécifier le réseau sur lequel l'IDS travaille. Il faut pour cela modifier la variable `HOME_NET` :

```
var HOME_NET [10.1.1.0/24] # SNORT travaille sur le réseau 10.1.1.0

var HOME_NET (10.1.1.0/24,192.168.1.0/24] # Si votre carte réseau possède 2 alias
```

Dans le fichier de configuration de SNORT (`/etc/snort/snort.conf`), vous avez toute une série de include. Il s'agit des règles utilisées par SNORT pour détecter d'éventuelles intrusions. Il y a des règles de telnet, ICMP, FTP, ... Bref, commentez celles que vous ne voulez pas et décommentez celles qui vous parait utile. Conseil : Décommentez les règles ICMP, car elles ne cessent pas de vous remonter des alarmes très souvent inutiles.

Pour des explications plus détaillées concernant les règles SNORT, allez voir ici.

Lancement de SNORT

Deux possibilités s'offrent à nous. Soit vous lancez SNORT tout seul, et dans ce cas, il génerera ces logs dans un fichier plat. Soit vous décidez de l'interfacer avec une base de données. Suivant le cas, SNORT ne se lancera pas de la même façon.

Sans Mysql :
```
/usr/local/snort*/src/snort −c /etc/snort/snort.conf −i eth0 −D
```

Avec Mysql :
```
/usr/local/snort*/src/snort −c /etc/snort/snort.conf
```

Remarque : Si vous souhaitez interfacer SNORT avec une base de données, ne lancez pas SNORT avec l'argument `−L` qui spécifie l'emplacement des logs.

Lier les logs SNORT avec MySQL

Maintenant, nous allons éditer le fichier de configuration de SNORT afin de lui indiquer qu'il faut rediriger les logs dans une base de données (ici MySQL). Avec vos yeux de lynx, retrouvez la ligne suivante dans le fichier de configuration SNORT `/etc/snort/snort.conf` :

#output database:log,mysql,user=root password=test dbname=SNORT host=localhost

Décommentez et modifiez cette ligne par :

output database:log,mysql,user=user_snort password=snort_pwd dbname=snort host=localhost

Ici, l'utilisateur MySQL accédant à la base de données s'appelle "user_snort", son password associé est "snort_pwd", le nom de la base MySQL utilisée par snort est "snort" et la machine qui fait tourner la base Mysql est la même que celle où SNORT tourne.

Création de la base de données SNORT

Au préalable, assurez−vous d'avoir installé :

PACKAGES	**REMARQUES**
`MySQL−client−*`	partie cliente de MySQL
`MySQL−devel−*`	

Astuce : La commande "rpm −qa | grep client" vous permet de vérifier que votre station Linux possède bien ces packages installés.

Suivez alors les instructions suivantes :

COMMANDES	**REMARQUES**
`cd /usr/local/snort*/contrib`	on se place à l'endroit du fichier contenant les tables SQL de SNORT
`mysql −u root −p`	Connexion à la base de données en tant qu'administrateur (au passage, si ce n'est pas encore fait, définissez un password pour l'administrateur de la base par la commande 'set password for root@localhost=PASSWORD('totomdp');
`create database SNORT;`	Création de la base de données SNORT
`use mysql;`	On se place ici pour créer l'utilisateur MySQL qui gérera la base de données snort
`insert into user values('localhost', 'user_snort', password('snort_pwd'), 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', '', '', '', '', 'Y', 'Y', 'Y');`	Création utilisateur MySQL "user_snort". Attention le nombre de 'Y' dépend de votre version de MySQL. (faites un `select * from user;` pour voir combien il faut en mettre)

`grant ALL PRIVILEGES ON SNORT.* TO user_snort@localhost IDENTIFIED BY 'snort_pwd' WITH GRANT OPTION;`	Attribution des droits de la base "snort" à l'utilisateur "user_snort"
`flush privileges;`	Recharge les tables de droits pour prendre en compte les nouvelles modifications
`use snort;`	on se place dans la base où l'on veut créer les tables pour SNORT
`Source create_mysql`	Création des tables pour SNORT

Vérifiez que les tables sont bien créées. Allez voir dans `/var/lib/mysql/snort` et vous y verrez tout un tas de fichiers correspondant au nom des tables de la base de données SNORT (il doit y avoir 3 fichiers par tables).

Lancez SNORT. Désormais, SNORT envoie les informations dans la base de données (astuce : installez PhpMyAdmin, et vérifiez la taille de la base de données SNORT. Si tout fonctionne, vous la voyez augmenter si bien évidemment il y a du trafic !).

Installation/Configuration ACID

ACID est une interface PHP qui permet de visualiser les remontées d'alarmes générées par SNORT. Cette partie sous−entend que vous avez une base de données qui récupère les informations envoyées par SNORT. Avant de suivre l'installation de cette application, assurez−vous d'avoir téléchargé :

- Adodb : Contient des scripts PHP génériques de gestion de bases de données. L'installer dans la racine d'apache (`/var/www/html/adodb par exemple`)
- PHPlot : librairie de scripts PHP utilisée par ACID pour présenter graphiquement certaines données statistiques (optionnel)

Le téléchargement de ACID se fait ici. Imaginons que la racine de votre serveur web est /var/www/html. Installez ACID dans la racine d'apache :

COMMANDES	**REMARQUES**
`cd /var/www/html`	Placez−vous dans la racine du serveur web
`tar −xvzf acid*`	Décompactage de ACID
`tar −xvzf adodb*`	Décompactage de AdoDB
`tar −xvzf phplot*`	Décompactage de PHPlot
`vi /var/www/html/acid/acid_conf.php`	Renseignez les champs suivants : ♦ `$DBlib_path="../adodb";` ♦ `$Chartlin_path="../phplot";` ♦ `alert_dbname="snort"` ♦ `alert_host="localhost"` ♦ `alert_user="user_snort"` ♦ `alert_password="snort_pwd"`

Voilà, maintenant vous pouvez vérifier que ACID est bien configuré (allez voir sur http://localhost/acid). Si vous le souhaitez, L'accès peut se faire via certificat SSL de manière à crypter l'échange entre vous et le détecteur d'intrusions.

Sachez que ce document a pour but de vous apporter quelques éléments de réponse concernant l'installation et la configuration de l'IDS SNORT. Il est loin d'être parfait. Vos remarques sont les bienvenues. Je prévois de modifier le présent document suivant les remarques que vous y apporterez.

Pour me contacter : guitarparts chez fr point st