



S E C U R I N E T S

Le club de la sécurité informatique

I N S A T

P r é s e n t e

Atelier

Prelude IDS

Formateurs:	Mabrouk Samy
	Abdelaali Dorra
	Gharbi Asma
	Naifer Abir
	Tounsi Wiem

1. Les IDS

Un IDS ou système de détection d'intrusions vient compléter les équipements et logiciels de sécurité (serveurs proxy, routeurs filtrants, firewalls...)

Les IDS permettent de collecter de façon automatisée les données représentant l'activité des systèmes (serveurs, applications, systèmes, réseaux), de les analyser et d'avertir les administrateurs en cas de détection de signes d'attaques.

1.1 Critères de classification des IDS

Par méthodes d'analyse

L'approche par scénario : consiste à rechercher dans l'activité de l'élément surveillé les empreintes d'attaques connues. Ce type d'IDS est purement réactif ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour fréquentes. De plus, son efficacité dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion" qui consistent à maquiller les attaques utilisées et ainsi elles ne sont plus reconnues par l'IDS.

L'approche comportementale : consiste à détecter des anomalies. La mise en œuvre comprend une phase d'apprentissage au cours de laquelle les IDS vont "découvrir" le fonctionnement "normal" des éléments surveillés et ensuite ils vont signaler les divergences par rapport au fonctionnement de référence. Ils présentent l'avantage de détecter des nouveaux types d'attaques.

Autres critères

Parmi les autres critères de classification existants, nous pouvons citer entre autres :

- les sources de données à analyser (réseau/système/application),
- le comportement de l'IDS après intrusion (passif/actif),
- la fréquence d'utilisation (périodique/continue).

1.2 Les différents types d'IDS

Les NIDS (Network IDS)

Ils analysent le trafic réseau ; ils comportent généralement une sonde qui "écoute" sur le segment de réseau à surveiller et un moteur qui réalise l'analyse du trafic afin de détecter les signatures d'attaques ou les divergences face au modèle de référence.

Deux problèmes majeurs: l'utilisation grandissante du cryptage, et des réseaux commutés

Il est d'une part plus difficile " d'écouter " sur les réseaux commutés et le cryptage rend l'analyse du contenu des paquets presque impossible.

Les HIDS

Ils analysent le fonctionnement ou l'état des machines sur lesquelles ils sont installés afin de détecter les attaques. Pour cela ils analysent les journaux systèmes, l'accès aux appels systèmes, vérifient l'intégrité des systèmes de fichiers ...

Ils sont très dépendants du système sur lequel ils sont installés. Il faut donc des outils spécifiques en fonction des systèmes déployés. Il faut cependant noter qu'ils sont incapables de détecter les attaques exploitant les faiblesses de la pile IP du système, typiquement les Défis de service.

Les IDS hybrides (NIDS+HIDS)

Combinaison de NIDS et HIDS. Ils permettent, en un seul outil, de surveiller les réseaux et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et corréler les informations d'origines multiples.

2. Prelude-IDS

Prelude-IDS est un système de détection d'intrusions et d'anomalies distribué sous licence GPL.

La détection d'intrusion est réalisée par l'analyse du trafic réseau et l'utilisation de signatures d'évènements hostiles ou par l'analyse en continue de fichiers de journalisation.

L'architecture de Prelude est :

- modulaire : intégrer ou développer de nouvelles fonctionnalités grâce à des plugins
- distribuée : Les composants sont autonomes et interactifs, (les sondes et les managers)
- sécurisée : utilisation du support SSL pour l'authentification et le chiffrement des communications.

Les sondes (réseaux comme locales) n'effectuent que les opérations de surveillance et de génération d'alertes alors que les managers prennent en charge la gestion des sondes et la journalisation des alertes.

2.1 Architecture de prelude :

Il s'agit en fait d'un IDS hybride, car il est composé de deux types de détecteurs ('sensors') qui tournent en daemon sur des machines hôtes :

- **prelude-nids**, offre la possibilité d'écouter le trafic réseau à la recherche d'un schéma d'attaque connu.

Pour analyser le trafic, prelude-nids utilise des règles (ou rules) dont la syntaxe se base sur celle utilisée pour les règles de Snort.

- **prelude-lml**, (Log Monitoring Lackey) analyse constamment les logs de la machine sur laquelle il est lancé, dans le même but que le premier.

Prelude-lml a pour but d'analyser constamment les nouvelles entrées dans le fichier syslog. Celui-ci offre notamment la possibilité de se comporter comme un daemon syslog (syslogd) pour pouvoir analyser les logs en provenance de diverses machines. Pour analyser ces logs, Prelude-lml utilise, comme prelude-nids, un ensemble de règles.

Ces sondes, lorsqu'elles détectent quelque chose, le rapportent immédiatement au manager.

- **prelude-manager** : Le manager est un autre daemon généralement associé à une base donnée mysql qui enregistre toutes les alertes données par les sondes.

Les sondes peuvent envoyer leurs alertes de différentes manières selon les possibilités qu'on leur offre: les deux principales possibilités étant soit par connexions ssl, soit par sockets Unix. Ces alertes sont envoyées dans le format IDMEF qui est propre à prelude basé sur le Xml.

Une fois l'alerte reçue, le manager peut soit simplement enregistrer celle-ci pour en faire part à l'administrateur, soit faire remonter l'information à un autre manager.

2.2 Pré-installation :

Il faut au préalable qu'un ensemble de paquetages et de bibliothèques soit installé :

Paquetage nécessaire	Versions utilisées pour notre installation
Gcc	gcc-4.0.0-8
libgpg-error	libgpg-error-1.0-2
libgpg-error-devel	libgpg-error-devel-1.0-2
Libgcrypt	libgcrypt-1.2.1-1
libgcrypt-devel	libgcrypt-devel-1.2.1-1
Gnutls	gnutls-1.0.25-1
gnutls-devel	gnutls-devel-1.0.25-1
Python	python-2.4.1-2
python-devel	python-devel-2.4.1-2
Pcre	pcre-5.0-4
pcre-devel	pcre-devel-5.0-4
Perl	perl-5.8.6-15
Mysql	mysql-devel-4.1.11-2
mysql-server	mysql-server-4.1.11-2
mysql-devel	mysql-4.1.11-2
Libpcap	libpcap-0.8.3-12
Cheetah (nécessaire pour l'installation de Prewikka)	Version 1.0

2.3 Mise à jour du système :

```
# yum update
```

Installation du framework Prelude-IDS :

- Télécharger les dernières sources stables à partir des adresses suivantes :
- <http://www.prelude-ids.org/download/releases/libprelude-latest.tar.gz>
- <http://prelude-ids.org/download/releases/libpreludedb-latest.tar.gz>

- <http://www.prelude-ids.org/download/releases/prelude-manager-latest.tar.gz>
- <http://www.prelude-ids.org/download/releases/prelude-lml-latest.tar.gz>

➤ Ajouter les chemins suivants dans le fichier */etc/ld.so.conf*

- /lib/tls
- /usr/local/bin
- /usr/local/lib

➤ Installation de libprelude

```
# tar -xvzf libprelude-latest.tar.gz
# cd libprelude-0.9.7.2
# ./configure
# make
# make install
```

De même pour les trois autres composants.

➤ Mettre à jour la liste des bibliothèques partagées (après chaque installation) :

```
# ldconfig
```

➤ Créer la base de données *prelude* et de l'utilisateur *securinets*.

```
mysql> CREATE database prelude;
mysql> GRANT ALL PRIVILEGES ON prelude.* TO securinets@'localhost' IDENTIFIED BY securinets;
```

➤ Création des tables :

```
# mysql -u securinets prelude -p </usr/local/share/libpreludedb/classic/mysql.sql
```

➤ Lister les tables

```
# mysql -u root -p
mysql> show databases;
mysql> use prelude;
mysql> show tables;
```

➤ Enregistrement de la sonde chez le manager

Pour enregistrer prelude-lml, lancer dans un premier Shell :

```
# prelude-adduser register prelude-lml "idmef:w admin:r" localhost
```

L'ordre "idmef:w admin:r" représentent les droits d'enregistrement de la sonde.

"idmef " correspond au format des alarmes, autoriser le droit en écriture est nécessaire pour que la sonde puisse écrire les alarmes au "manager "

"admin:r " correspond aux ordres administratifs envoyés au manager, les droits de lecture sont suffisants.

Et dans un deuxième Shell :

```
# prelude-adduser registration-server prelude-manager
```

Le manager va générer un « one-shot password » servant la sonde à s'enregistrer chez lui.

Après avoir suivi les étapes prescrites sur écran, la phrase suivante sera affichée sur le terminal sonde :
prelude-lml registration to localhost successful

➤ Test de fonctionnement :

Nous supposons dans cet exemple que la sonde et le manager se trouvent dans la même machine. Autrement, il suffit de changer 'localhost' par l'adresse adéquate ou manipuler les fichiers de configuration.

Pour mettre le prelude-manager en écoute, taper dans le shell correspondant:

```
# prelude-manager --prelude --listen =127.0.0.1 --db --type=mysql --name prelude --textmod=stderr
```

On verra s'afficher le numéro de port (*nport=4690 par défaut*) sur lequel écoute le prelude-manager.

Ce numéro permet à prelude-lml de se connecter à son tour au manager via la commande :

```
# prelude-lml --prelude --profile=prelude-lml --server-addr=localhost :nport
```

3. Prewikka

Est l'interface graphique associée à Prelude-IDS permettant d'accéder aux alertes générées. et de réaliser un tri et un filtrage selon les requêtes d'interrogation SQL sous-jacentes

La visualisation est simple et a lieu sur un navigateur Web et un serveur HTTP.

3.1 Sources:

Télécharger

- Prewikka : <http://www.prelude-ids.org/download/releases/prewikka-latest.tar.gz>
- cheetah : <http://www.cheetahtemplate.org/>

3.2 Installation:

- cheetah

```
tar -xvf cheetah-latest.tar.tar
cd cheetah-2-0rc7
python setup.py install
```

- prewikka

```
tar -zxvf prewikka-latest.tar.gz
cd prewikka-0.9.0-rc5
python setup.py install
```

3.3 Création de la base de données Prewikka :

Création de la BD:

Créer une nouvelle base de données appelée 'prewikka' :

```
mysql> CREATE database prewikka;
```

Créer un utilisateur sur la base préwikka :

Créer un nouvel utilisateur 'prewikka' avec un password 'prewikka' qui va accéder à la base 'prewikka', mais uniquement à partir de localhost :

```
GRANT ALL PRIVILEGES ON prewikka.* TO prewikka@'localhost' IDENTIFIED BY 'password';
```

Création des tables

```
$ mysql -u prewikka prewikka -p < /usr/share/prewikka/database/mysql.sql
```

Enter password:

3.4 Editer prewikka.conf:

Après la création de la base de données pour prewikka, on doit éditer /etc/prewikka/prewikka.conf pour adapter les paramètres de la base.

```
[interface]
#This is the name at the top right and left of the Prewikka interface
#You can change it or leave as is
software: Prewikka
place: company ltd.
title: Prelude management

#The following are the setting for your prelude database
[idmef_database]
type: mysql
host: localhost
user: securinets
pass: securinets
name: prelude

#This is the database information for the prewikka DB you created above
[database]
type: mysql
host: localhost
user: prewikka
pass: prewikka
name: prewikka
```

3.5 Lancement de Prewikka à partir de Apache web server

Editer le fichier : /etc/httpd/conf/httpd.conf et ajouter le code suivant :

```
<VirtualHost *:8000>
ServerName my.server.org
Setenv PREWIKKA_CONFIG "/etc/prewikka/prewikka.conf"
```

```
<Location "/">
  AllowOverride None
  Options ExecCGI

  <IfModule mod_mime.c>
    AddHandler cgi-script .cgi
  </IfModule>

  Order allow,deny
  Allow from all
</Location>

Alias /prewikka/ /usr/share/prewikka/htdocs/
ScriptAlias /usr/share/prewikka/cgi-bin/prewikka.cgi

</VirtualHost>
```

Maintenant, lancer prewikka-httpd et ouvrir le browser en entrant dans la barre d'adresse:
<http://localhost:8000>

Si tout va bien, on verra l'interface 'prewikka' apparaître sur scène !!