Présentation Prelude IDS 0.9-cvs OSSIR

Support de la conférence de l'OSSIR du 11 juin 2002

Guillaume Arcas – guillaume.arcas@free.fr

Plan

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

1. Introduction

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

Un tel système vient compléter la panoplie des équipements et logiciels de sécurité (routeurs filtrants, serveurs proxy, pare-feux...) et offre à l'exploitant Sécurité et/ou l'analyste un outil de contrôle des activités suspectes ou illicites (internes comme externes).

L'architecture modulaire et naturellement distribuée de Prelude permet de n'installer que ce qu'il faut là où il faut, sans surcharger le réseau ni les systèmes hôtes.

Grâce à des sondes dédiées, il autorise la prise en compte au sein d'un schéma unique et homogène, de la quasi-totalité des évènements de sécurité, que cela soit au niveau réseau (network-based detection) ou local (host-based detection).

La détection d'intrusions est réalisée par analyse du trafic réseau et l'utilisation de signatures (en l'occurrence celles de Snort) d'évènements réputés hostiles ou par l'analyse en continu de fichiers de journalisation (sur les serveurs où ont été installées des sondes locales) et l'utilisation d'expressions régulières PERL (ce qui permet la rédaction de règles propres à tel ou tel format de fichier ou à telle ou telle application).

Plus - et mieux - qu'hybride (synonyme de disparate) Prelude-IDS est un système complet.

Note : la version présentée dans ce document est la "0.9 CVS" (le CVS étant plus important que le 0.9) du 04 juin 2002. L'utilisation de la version 0.4.2 est à proscrire...

2. Présentation

2.1. Une architecture ...

Nous avons dit dans l'introduction de l'architecture de Prelude-IDS (que nous n'appellerons plus par la suite que Prelude pour faire plus court...) qu'elle est modulaire et distribuée.

2.1.1. modulaire ...

L'architecture Prelude est modulaire en ce sens que ses composants (prelude-manager, prelude-nids, prelude-lml) et la librairie libprelude sur lesquels ils s'appuient, intègrent nativement la notion de "plugin". Cela permet - nous aborderons concrètement ce point plus loin - d'étendre les fonctionnalités de base des composants grâce au développement de modules spécialisés ou d'en incorporer de nouvelles.

2.1.2. distribuée ...

Le caractère distribué d'un IDS construit au-dessus de Prelude est un fait qu'il ne faut jamais perdre de vue lorsque l'on déploie des composants Prelude.
A l'inverse d'un autre produit issu du libre plus célèbre, Prelude est bien une suite de composants et non un logiciel monolithique.
Les composants Prelude - sondes et managers - ont été pensés et développés pour être autonomes (donc légers car dédiés à une tâche) et interactifs (les uns ne fonctionnent pas sans les autres).

Ainsi les sondes - réseau comme local - n'effectuent que les opérations de surveillance et de génération des alertes.
Les managers quant à eux prennent en charge la gestion des sondes et la journalisation des alertes. Dans certains cas, ils peuvent également ne prendre en charge que le routage des alertes vers d'autres managers (relay). Enfin, ils peuvent être utilisés pour déclencher des actions de contre-mesure au niveau d'un sous-réseau particulier tout en assurant la remontée des alertes vers les contrôleurs de niveau supérieur.

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

Cela se traduit en pratique par la possibilité d'installer autant de sondes et de contrôleurs que souhaité ou nécessaire, afin d'assurer la redondance des composants et/ou de s'adapter à la charge et la complexité d'un réseau, tout en ayant l'assurance d'obtenir *in fine* une journalisation centralisée dans un format homogène.

2.1.3. sécurisée ...

Le "modèle de sécurité" de Prelude est un des points forts du produit.

Tous les composants sont construits au-dessus de la librairie libprelude qui peut être compilée avec le support SSL (utilisant les fonctions fournies par la suite openSSL).
Ce support permet deux choses :
- une authentification "forte" des composants entre eux ;
- le chiffrement des communications entre composants.

L'authentification des sondes par les managers est donc effectuée sur la base de certificats et le transfert des messages entre ces composants bénéficie du chiffrement.

Cela signifie qu'il est possible de :
- déployer un IDS Prelude sur des sous-réseaux distants reliés entre eux par des canaux non sûrs (comme Internet) tout en conservant la possibilité de centraliser la journalisation des alertes ;
- ne pas avoir à installer un LAN dédié à la détection d'intrusions sur les réseaux concernés par l'IDS.

Si les sondes n'intègrent pas le support SSL (librairies non disponibles sur les systèmes hôtes ou réseau supposé sûr), il est possible de sécuriser la remontée des alertes vers un site central : suffit que le dernier manager-relay supporte SSL pour que les alertes puissent en toute quiétude transiter par Internet.

Quoiqu'il en soit, pour être prise en compte par un manager, une sonde doit au préalable avoir été déclarée - enregistrée - auprès de celui-ci.
Dans le cas de sondes et managers supportant SSL, cela se traduit par la génération d'une clef privée sur la sonde et d'un certificat sur le manager qui la prendra en compte.
Dans le cas d'une sonde ou d'un manager ne supportant pas ce mécanisme, cela se traduira par un simple échange de mot de passe, et les communications entre la sonde et le manager se feront en clair.

Dans tous les cas, il n'est pas possible de "polluer" un manager en installant une sonde "pirate".

2.1.4. ouverte ...

Le processus de journalisation peut être découper en deux parties :
- les sondes génèrent à partir des règles et signatures qu'elles intègrent des alertes ; ces alertes sont produites dans un format binaire IDMEF (voir plus bas) puis envoyées à un ou plusieurs managers.
- les managers traduisent les alertes reçues en un format lisible : soit en mode texte (journalisation fichiers) soit en mode SQL (utilisation d'un backend SGBD).

Si un mode alternatif doit être implémenté, cela peut être fait sous forme de plugin additionnel.

Prelude ayant été conçu pour prendre en charge des alertes de type et d'origine différents, il fallait choisir un format de journalisation permettant de traiter de la même façon et avec le même degré de précision les traces d'évènements réseau captés par les sondes de ce type tout comme celles extraites des fichiers de journalisation système ou application.

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

Le format IDMEF - encore au stade de draft - a été choisi pour son caractère ouvert et extensible. Afin de ne pas ralentir les processus de communication des alertes entre les sondes et les managers, une forme binaire de ce format est utilisée par Prelude, seuls les managers assurant la traduction finale des alertes dans un format lisible (texte ou SQL).

2.1.5. fiable ...

Si pour une raison ou une autre une sonde n'arrive plus à envoyer ses alertes à un manager auprès duquel elle est enregistrée, ces dernières sont conservées localement jusqu'à rétablissement de la connexion avec un manager. Cette fonctionnalité est fournie par la librairie libprelude, brique de base de tout composant Prelude.

2.1.6. et extensible.

A tous les niveaux ou presque il est possible d'étendre les capacités des composants Prelude à l'aide de module additionnel (plugin).

Ces modules peuvent ainsi :
- au niveau des sondes : assurer le support de nouveaux protocoles ou d'applications ;
- au niveau des managers : permettre un mode alternatif de journalisation.

Il est également possible d'étendre les capacités et fonctionnalités de l'IDS en intégrant d'autres produits (exemple : des sondes plus performantes, des programmes plus spécifiques, etc…) toujours grâce à la librairie libprelude. Ont ainsi été intégrées à Prelude les sondes Snort et FireStorm.

2.2. OS Supportés

Prelude a initialement été développé pour les systèmes de type Unix. L'intégration de systèmes du monde Microsoft peut actuellement s'effectuer grâce à un utilitaire comme ntsyslog qui permet la remontée d'alertes locales vers uns sonde prelude-lml simulant un serveur syslog. Cependant, la compilation des composants Prelude - ou tout au moins la sonde locale - pour systèmes Microsoft devrait faire partie des prochaines évolutions du produit.

Testés sur :
- Red Hat / Linux 7.0 et 7.2 ;
- Mandrake Linux 8.0 ;
- GNU/Debian 2.2

Annoncés comme fonctionnant sur :
- FreeBSD 4.5 et 4.6 ;
- OpenBSD 3.1 (non mais ! ! ☺)
- Sun Solaris.

Testés mais non stabilisés :
- MS Windows NT/2000 – Cygwin.

2.3. Composants

Prelude se compose de quatre sous-ensembles :
- la librairie libprelude ;
- la sonde réseau prelude-nids ;
- la sonde locale prelude-lml ;
- le contrôleur prelude-manager ;
- le frontal web prelude-php-frontend.

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

2.3.1. La librairie Prelude (libprelude)

La librairie libprelude constitue la brique de base de tout composant Prelude (à l'exception du frontal web).

Cette libraire fournit aux composants Prelude les fonctionnalités suivantes :
- gestion de la connexion entre composants (sondes et managers) notamment le mécanisme de reprise après interruption et de rétablissement automatique de la connexion ;
- gestion du mode de communication entre composants, notamment la prise en charge du chiffrement éventuel et de l'authentification ;
- interface permettant l'intégration de modules additionnels (plugins).

Cette librairie doit être installée préalablement à l'installation de tout autre composant (à l'exception du frontal web).

2.3.2. La sonde réseau (prelude-nids)

Cette sonde prend en charge l'analyse en temps réel du trafic réseau "à la snort".

Elle est construite au-dessus de la librairie libprelude, et fournit :
- un moteur de gestion de signatures générique, actuellement compatible avec les signatures Snort, mais pouvant être étendu par l'ajout de nouveaux "parsers" de règles.
- des modules spécialisés par protocoles : par exemple, un plugin est dédié aux protocoles RPC et permet l'analyse fine de ce type de connexions. D'autres permettent le décodage des requêtes HTTP, des séquences UTF-8, des sessions FTP ou telnet.
- des modules spécialisés dans la détection non basée sur des signatures : détection des activités de balayage (scan), de "spoofing" ARP, détection des tentatives d'échappements Shell (ShellCode).

Les sondes réseau peuvent aussi prendre en charge la défragmentation IP et le réassemblage des flux TCP, de façon à rendre une sonde réseau Prelude moins vulnérable aux "attaques" de type Stick ou Snot.

2.3.3. La sonde locale (prelude-lml)

Cette sonde prend en charge la remontée d'alertes détectées localement (host based detection) sur une machine. Cette détection est actuellement basée sur l'application à des objets déterminés (fichiers de journalisation système et/ou application) de règles construites autour d'expressions régulières compatibles Perl (PCRE).

Pour la surveillance des systèmes Unix, une sonde prelude-lml peut jouer le rôle d'un serveur syslog, et ainsi assurer la remontée d'alertes en provenance de plusieurs serveurs sur lesquels il suffira de modifier le comportement de syslog en conséquence.
L'intégration des systèmes du monde Microsoft peut également se faire à l'aide de l'utilitaire ntsyslog.

Un message est généré par la sonde prelude-lml dès qu'une ligne de log correspond à une expression régulière.

2.3.4. Le contrôleur (prelude-manager)

Prelude-manager centralise les messages des sondes réseaux et locales et les traduit en alertes.
Il est responsable de la centralisation de la journalisation à travers deux fonctions :
- celle de relais : un contrôleur relais va assurer le routage vers un contrôleur maître (ou un autre relais dans le cas d'architecture en cascade) d'alertes provenant des sondes qui lui sont rattachées.
- celle de maître : un tel contrôleur va assurer la réception des messages et alertes provenant des sondes et/ou des contrôleurs relais qui lui sont rattachés ainsi que leur journalisation dans

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

un format unique et lisible par l'analyste : en mode texte (dans des fichiers) ou SQL dans le cas de l'utilisation d'un SGBD (actuellement sont supportés MySQL et PostgreSQL).

Un contrôleur Prelude assure également la remontée des tests de connexion (" heartbeats ") échangés avec les sondes réseaux et locales. Ces tests permettent de vérifier la continuité de la communication entre sondes et contrôleurs.

Le contrôleur est peut-être le composant le plus important d'un IDS à base de Prelude, pour plusieurs raisons :

- pas de journalisation possible sans (au moins) un contrôleur ;
- il est possible d'étendre les capacités d'un contrôleur à l'aide de plugins, que cela soit en introduisant des nouveaux formats de journalisation des alertes (actuellement les modes texte et insertion SQL sont supportés nativement, mais on pourrait envisager de réintroduire les modes HTML et XML par exemple) ou en autorisant le traitement de messages en provenance de composants autres que Prelude, un contrôleur Prelude pouvant ainsi – simple exemple - centraliser la remontée d'alarmes en provenance de sondes Snort…

Autre fonctionnalité proposée par les contrôleurs Prelude : la possibilité de récupérer via un port d'administration les options avec lesquelles s'exécutent les sondes.
Ces échanges entre contrôleurs et sondes se font actuellement à sens unique (remontée des options des sondes vers un contrôleur) mais il est prévu dans un futur - que l'on espère très proche - qu'ils se fassent dans les deux sens, ce qui permettra la modification, depuis une console d'administration, du comportement des sondes, et en particulier l'activation de nouvelles règles de filtrage et de nouvelles signatures.

2.3.5. L'interface web (prelude-php-frontend)

Enfin - at last but not least - Prelude ne serait pas un produit complet s'il ne proposait pas une interface de visualisation des alertes : prelude-php-frontend.

Cette interface composée de scripts PHP est destinée à être installée sur un serveur web de type Apache indépendamment des autres composants Prelude.

Cela signifie que l'installation préalable de la librairie libprelude est inutile, mais que par contre celle d'un serveur web supportant PHP 4 l'est !

L'interface Prelude étant une console permettant de consulter la base de données, cela signifie également que le mode SQL doit avoir été choisi comme mode de journalisation des alertes.

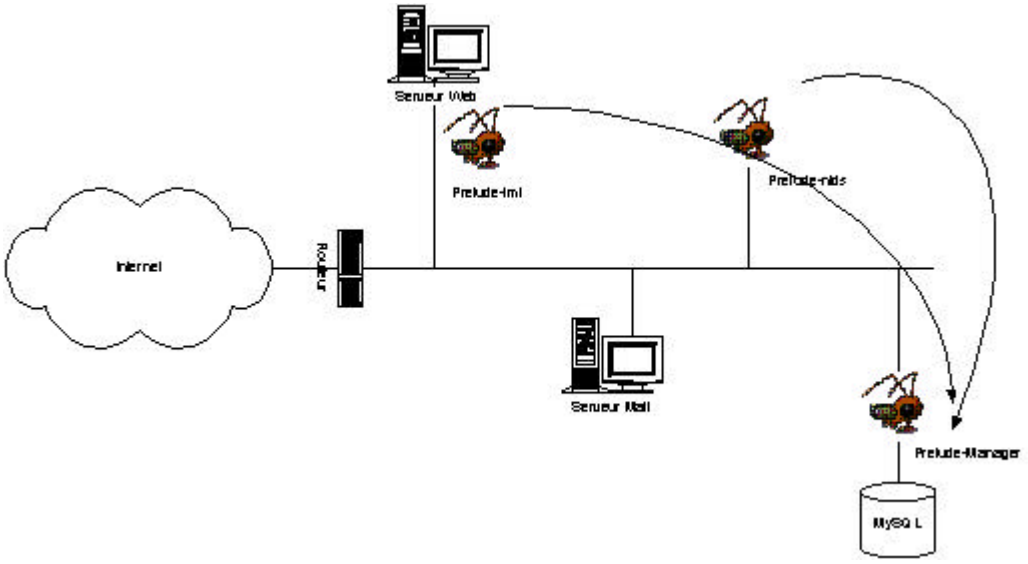
L'utilisation de PHP comme langage de développement de l'interface permet d'étendre facilement les fonctionnalités de base.

2.4. Aperçu

Déployé sur un seul réseau, un IDS Prelude ressemble à ceci :

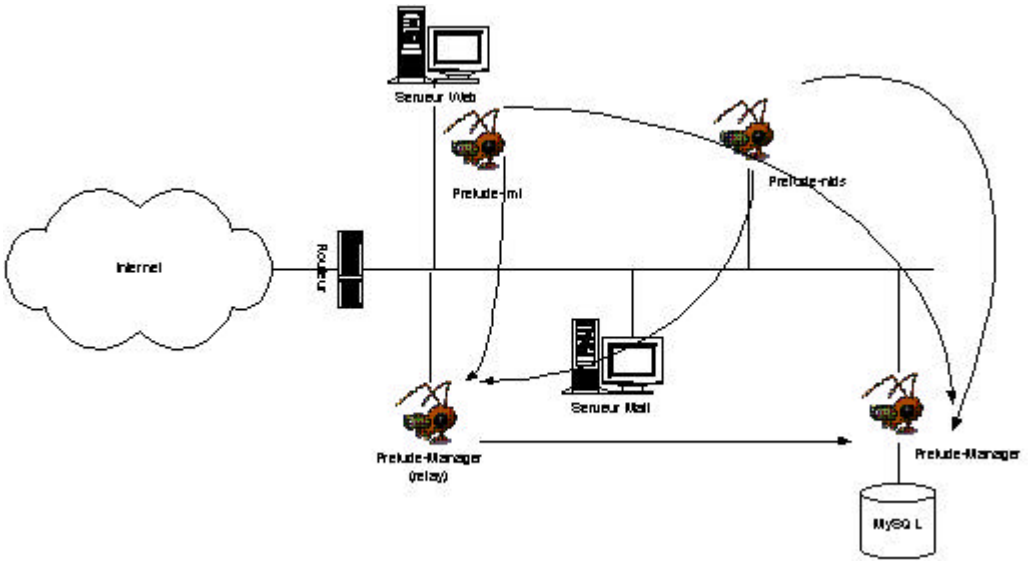
© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.



Dans cette configuration, des sondes (locales et réseau) envoient des messages à un contrôleur qui se charge de leur journalisation dans une base SQL. (L'interface web peut elle être installée sur cette même machine ou ailleurs). Le trafic entre les composants Prelude est chiffré et authentifié.

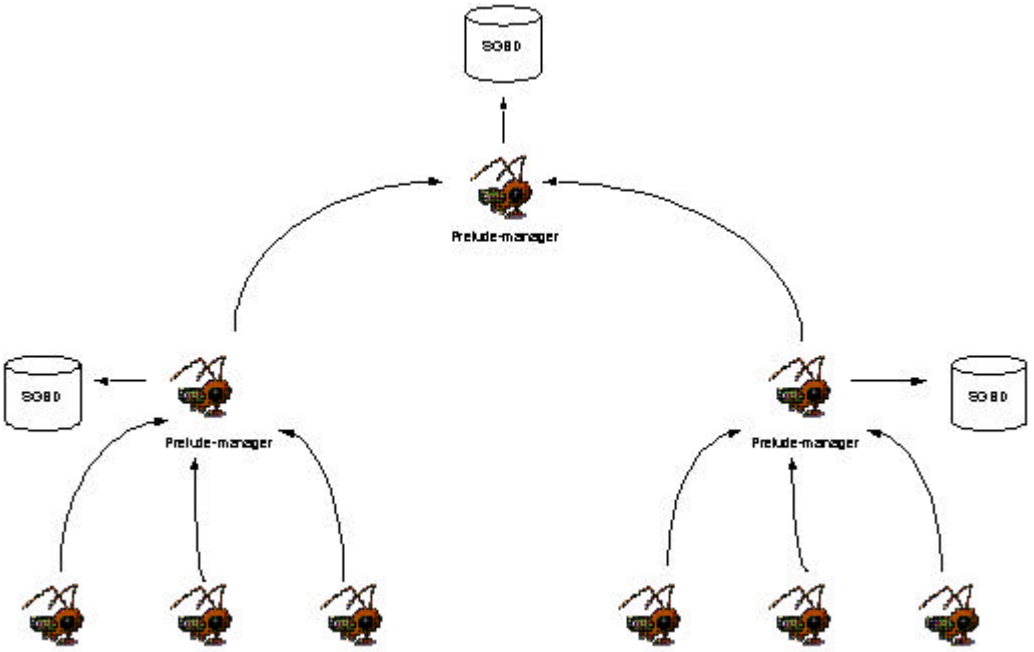
On peut renforcer la qualité du service en ajoutant un second contrôleur qui servira de backup en cas d'indisponibilité du premier :



Dans cette extension de la configuration précédente, nous disposons maintenant d'un contrôleur relais : celui-ci pourra continuer de router les messages en provenance des sondes vers le contrôleur principal ou « spooler » ceux-ci le temps que la connexion soit rétablie avec le contrôleur principal, déchargeant les sondes de cette tâche (spool).

Note : les contrôleurs peuvent être déployés en cascade de la manière suivante :

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.



Dans le schéma ci-dessus, les sondes (composants de plus bas niveau) locales comme réseau sont reliées à un contrôleur (prelude-manager). Ce contrôleur assure deux fonctions :
- journalisation dans une base SQL des alertes remontées par les sondes ;
- reroutage des messages de ces mêmes sondes vers un contrôleur de niveau supérieur.

Cette configuration peut être adaptée à une organisation disposant de sites distants et désirant donner les moyens à une équipe Sécurité Réseaux locale de gérer ses propres évènements, tout en donnant les moyens à une équipe du site central d'analyser les évènements de tous les sites locaux afin d'y chercher et d'y découvrir des constantes ou des redondances permettant d'identifier des attaques spécifiques lancées non contre un site mais contre l'ensemble des sites de l'organisation.
Passons maintenant à la pratique.

3. Installation

L'installation des différents composants Prelude est relativement simple puisqu'elle repose, après extraction de l'archive, sur la désormais célèbre trilogie " configure - make - make install " depuis la version 0.9.

Cette simplicité ne doit pas faire oublier que Prelude est avant tout destiné à implémenter un IDS distribué, et qu'il peut d'avérer très utile de passer par une phase d'analyse approfondie de sa future architecture, de façon à installer ce qu'il faut là où il faut. Ceci dit, il est très facile d'étendre - nous le verrons plus loin dans l'étude de cas - une architecture au départ simple par l'ajout de composants.

3.1. Installation de la librairie libprelude

Rappelons que l'installation de la librairie Prelude doit se faire préalablement à celle de tout autre composant (à l'exception de l'interface web).

L'installation de la librairie Prelude n'échappe pas à la règle énoncée ci-dessus :
```
- configure  (par défaut, s'installe sous /usr/local).
- make
- su
- make install
```

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

A l'issue de l'installation, les librairies sont installées (ce qui est somme toute logique, le contraire en eût étonné plus d'un !) et un répertoire prelude-sensors a été créé, dans lequel un fichier de configuration par défaut (sensors-default.conf) a été installé.

Durant la phase d'installation, le support SSL aura ou non été pris en compte selon que les librairies OpenSSL requises auront ou non été trouvées.

Un utilitaire - sensor-adduser - est également présent dans `/usr/local/bin`. Il sera utilisé pour enregistrer les composants Prelude auprès des contrôleurs.

Vous ne devriez pas rencontrer trop de problème à ce stade de l'installation...

3.2. Installation d'un contrôleur

Compte-tenu de l'architecture distribuée de Prelude, il peut être intéressant de commencer le déploiement de l'IDS par l'installation d'un ou plusieurs contrôleurs (prelude-manager).

Une fois encore, la procédure est simple :
- `configure (par défaut, s'installe sous /usr/local).`
- `make`
- `su`
- `make install`

En plus du binaire, un fichier de configuration (prelude-manager.conf) est installé dans `/usr/local/etc/prelude-manager`.
Ce fichier déterminera le comportement du contrôleur :
- adresse et port d'écoute ;
- activation des modules de sorties (fichier texte ou insertions SQL).

L'activation des modules et agents de contre-mesure sera également configurée dans ce fichier.

Notez que si vous décidez d'utiliser une base de données (MySQL ou PostgreSQL) pour journaliser les alertes Prelude, il vous faudra :
- disposer d'un SGBD ;
- lancer le script prelude-manager-db-create.sh qui, comme son nom le laisse deviner, va créer les bases de données nécessaires.

Deux solutions :
- soit le SGBD est installé sur le même hôte que le contrôleur (ou vice versa...) ;
- soit le contrôleur communiquera avec lui via le réseau.

La première de ses solutions est souhaitable dans le cas de contrôleurs supportant SSL, car elle garantit que les communications entre les sondes jusqu'à la journalisation sont chiffrées.

Si vous n'utilisez pas de SGBD pour journaliser les alertes, vous ne pourrez pas bénéficier de l'interface web prelude-php-frontend d'une part et vous devrez paramétrer la rotation des fichiers de journalisation.

Enfin, en plus du binaire prelude-manager est installé l'utilitaire manager-adduser, dont nous détaillerons plus loin le fonctionnement et qui est nécessaire à l'enregistrement des sondes auprès du contrôleur.

3.3. Installation d'une sonde réseau

Une fois la libraire Prelude installée, l'installation d'une sonde réseau se déroule suivant le même principe :
- `configure (par défaut, s'installe sous /usr/local).`

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

```
- make
- su
- make install
```

A l'issue, le binaire prelude-nids est installé dans `/usr/local/bin` (sauf directive contraire lors de l'exécution du configure...) et les fichiers de configuration de la sonde réseau se trouvent sous `/usr/local/etc/prelude-nids`.
On y trouvera les fichiers suivants :

- prelude-nids.conf : paramètres de configuration affectant le comportement de la sonde (adresse et port d'écoute du ou des contrôleurs vers lesquels la sonde enverra ses messages, configuration du réassemblage des flux TCP, modules de détection activés...). Par défaut, les modules de détection SnortRules (compatibilité avec les règles et signatures Snort), ScanDetect (comme son nom l'indique...), HttpMod (normalisation des requêtes HTTP, RpcMod (surveillance des services du même acabit) et TelnetMod sont activés.
- unitable.txt : une table de conversion Unicode / ASCII, utilisée par le module HttpMod en particulier.
- les règles Snort, dans le répertoire ruleset. A noter - mais nous y reviendrons - que le fichier classification.config fourni avec Prelude a été modifié pour répondre aux spécificités IDMEF.

3.4. Installation d'une sonde locale

Une sonde locale s'installe de la même façon qu'une sonde réseau :

```
- configure (par défaut, s'installe sous /usr/local)
- make
- su
- make install
```

En plus du binaire (que l'on trouvera sous `/usr/local/bin`), les fichiers de configuration suivants sont installés sous `/usr/local/etc/prelude-lml` :

- prelude-lml.conf : définit les paramètres généraux tels que l'adresse des contrôleurs associés à la sonde ou le port sur lequel la sonde doit écouter pour simuler un serveur syslog, les objets (fichiers) à surveiller, et déclare les modules de détection (actuellement SimpleMod).
- un répertoire ruleset contenant les règles (sous forme d'expressions régulières compatibles Perl, PCRE) de filtrage qui déclencheront l'envoi de messages par la sonde (des fichiers de filtres prêts à l'emploi sont fournis pour les logs syslog, cisco, netfilter...

3.4.1 Intégration des systèmes MS Windows NT/2000

Les hôtes MS Windows NT/2000, dans l'attente de la sortie des binaires Prelude pour ces systèmes, peuvent être intégrés à l'IDS grâce aux client syslog pour NT/2000 ntsyslog.
Cet utilitaire s'exécute comme un service NT et permet la remontée de messages vers un ou plusieurs serveurs de journalisation dans un format syslog :

```
Oct 18 21:37:34 test1.sabernet.net security[success] Successful Logon: User
Name:Administrator Domain:TEST1 Logon ID:(0x0,0x36D166) Logon Type:7 Logon
Process :User32 Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Work station Name:TEST1
```

De cette manière, les remontées d'alertes en provenance de ces systèmes s'effectueront via les sondes locales.

3.5. Installation de l'interface web

Seul composant à pouvoir être installé indépendamment de la librairie Prelude, prelude-php-fronted est une suite de scripts PHP implémentant une interface sobre mais complète de visualisation des logs Prelude.

Son installation nécessite :

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

- que l'on dispose d'un serveur web compatible PHP4 (Apache mais aussi IIS) ;
- que PHP4 (version 4.2.1 conseillée) y soit installé et configuré ;
- que l'on installe les librairies PHP AdoDB (interface générique bases de données, ce qui permet à l'interface Prelude de se " plugger " indifféremment sur un SGBD MySQL ou PostgreSQL, en attendant les plugins Oracle...) et PHPlot (permettant de générer des graphes de type camembert).

L'installation se fait simplement en extrayant l'archive sous la DocumentRoot du serveur web, éventuellement en déclarant un nouvel hôte virtuel.

Le script prelude-db-create.sh peut être lancé pour créer la base prelude-frontend (nom par défaut) dans laquelle seront stockées les préférences Utilisateur (mot de passe en particulier) et les définitions des présentations personnalisées.

Nous sommes à ce stade prêts pour passer à l'étape suivante : la configuration et le lancement des différents composants sur leurs systèmes hôtes.

4. Configuration

Une fois les différents composants installés, il va falloir les configurer pour mettre en œuvre l'IDS.

Le plus simple est de commencer par configurer un premier contrôleur et choisir un mode de journalisation.

4.1. Configuration du contrôleur

Un contrôleur Prelude se configure à l'aide du fichier prelude-manager.conf.

Ce fichier est typiquement divisé en deux parties :
- la configuration des paramètres réseau : adresse et port sur lesquels le contrôleur va se mettre à l'écoute des messages en provenance des sondes, adresses des contrôleurs de niveau supérieur vers lesquels le contrôleur va rerouter les messages qu'il reçoit.

Le paramètre relay-manager peut en effet accepter plus d'une adresse de relais sous la forme suivante :

```
relay-manager = x.x.x.x || y.y.y.y
```

Si le contrôleur d'adresse x.x.x.x est pour une raison ou une autre inaccessible, le contrôleur relais routera les messages vers le contrôleur d'adresse y.y.y.y. En cas d'échec, les messages ne sont pas perdus : ils sont conservés localement pour réexpdition ultérieure, dès qu'un des contrôleurs sera de nouveau joignable.

- la configuration des modules de sortie, actuellement au nombre de deux (les deux modes de journalisation HTML et XML ayant été abandonnés) : soit en mode texte dans un fichier (par défaut `/var/log/prelude.log`) soit dans une base de données (les SGBD MySQL et PostreSQL étant actuellement supportés).

Configurer un contrôleur revient donc :
- à déterminer quel type de contrôleur on va installer (relais ou non);
- à choisir un mode de journalisation (texte ou SQL).

Notez que le fait de configurer un contrôleur en tant que relais ne l'empêche pas de se voir attribuer un rôle actif (notamment dès que les modules de contre-mesure seront opérationnels) ou secondaire (un contrôleur relais peut tout à fait router des messages vers un contrôleur de niveau supérieur et en conserver une trace en local).

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

4.2. Configuration d'une sonde réseau

Une sonde réseau est configurée par l'intermédiaire du fichier prelude-nids.conf.

Ce fichier comprend les paramètres de connexion, notamment l'adresse et le port du ou des contrôleurs auxquels la sonde est rattachée. Optionnellement, on peut y préciser le nom d'utilisateur sous lequel doit s'exécuter la sonde.

Viennent ensuite les sections spécifiques pour chaque module :
- Tcp-reasm : prise en charge du réassemblage des flux TCP, de façon que seuls soient analysés les paquets faisant partie d'une session, l'objectif étant de rendre la sonde insensible aux attaques de type Stick ou Snot.

Exemple :

```
# TCP stream reassembly option
#
# Only analyse TCP packet that are part of a stream,
# this defeat stick/snot against TCP signatures.
statefull-only;

# Only reassemble TCP data sent by the client (default).
client-only;

# Only reassemble TCP data sent by the server.
# server-only;

# Reassemble TCP data sent by client and server.
# both;

# Only reassemble data to specific port (default is to reassemble everything).
# If this option is used with the statefull-only option, packet that are not
# going to theses specified port will be analyzed anyway.
port-list = 20 21 22 25 80;
```

- SnortRules : chemin d'accès aux fichiers de signatures Snort.
Prelude est en effet compatible avec les signatures et règles Snort, à cette différence près que le format du fichier classification.config a été modifié pour être adapté au format IDMEF.
Il est tout à fait envisageable d'incorporer à Prelude des décodeurs pour d'autres signatures par le biais de plugins.

4.2.1. Règles et signatures Snort

Pour ceux qui n'en auraient pas encore vue, une règle Snort ressemble à ceci :

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"EXPLOIT netscape 4.7
unsucessful overflow"; content: "|33 C9 B1 10 3F E9 06 51 3C FA 47 33 C0 50 F7
D0 50|"; flags: A+; reference:arachnids,214; classtype:unsuccessful-user;
sid:311; rev:2; reference:bugtraq,822;)
```

La première partie commence par un mot-clef (ici : alert) qui détermine ce que doit être le comportement de la sonde lorsqu'un paquet correspond à la règle (ici : émettre une alerte, soit, dans le contexte Prelude, envoyer à un contrôleur un message IDMEF au format binaire), suivi de la désignation du protocole (tcp), de l'origine du paquet ($HOME_NET étant ici une variable correspondant à la classe d'adresse locale), du port source (any signifiant littéralement n'importe quel port), une représentation fléchée du sens de la communication (-> étant synonyme de vers), puis se termine par la désignation des adresse et port de destination (ici le port 80 d'une adresse externe).

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

Viennent ensuite entre parenthèses l'intitulé de l'alerte, une partie en format hexadécimal du contenu du paquet, la position des drapeaux TCP, la classification et des références (généralement un renvoi vers un site web décrivant précisément le type d'attaque ou d'anomalie correspondant à l'alerte).

Il existe ainsi actuellement plusieurs centaines de signatures Snort prêtes à l'emploi.

- ScanDetect : détection des activités de balayage.

4.3. Configuration d'une sonde locale

Une sonde locale prend ses paramètres de configuration dans le fichier prelude-lml.conf.

Comme pour les composants vus précédemment, ce fichier comprend une première section définissant l'adresse des contrôleurs auxquels est rattachée la sonde. Particularité de la sonde locale : elle peut simuler un serveur syslog :

```
# [Udp-Srvr]
#
# port = 514
# addr = 0.0.0.0
```

Dans ce cas, les hôtes pris en charge doivent être configurés de telle façon que leur client syslog communique par le réseau et non plus seulement en local.

Vient ensuite la liste des objets locaux à surveiller :

```
file = /var/log/auth.log
file = /var/log/messages
file = /var/log/apache/access.log
```

Il s'agit des fichiers auxquels la sonde devra appliquer les règles définies dans la section suivante :

```
[SimpleMod]
ruleset=/usr/local/etc/prelude-lml/ruleset/simple.rules;
```

4.3.1. Règles de filtrage Perl

Une règle est une expression régulière qui, lorsqu'une ligne d'un des fichiers surveillés y correspond, déclenchera l'envoi d'un message par la sonde.

Une règle est définie par :

- une expression régulière compatible Perl qui va déclencher l'émission d'un message ;
- une référence ;
- l'origine de cette référence : unknown, bugtraqid, cve, vendor-specific.
- l'URL à laquelle on pourra consulter des informations complémentaires ou détaillées sur l'alerte.
- un indice de sévérité : low, medium, high.
- un indice d'impact : failed, succeeded.
- un type : admin, dos, file, recon, user, other.
- la description du type ;
- l'adresse (ou les adresses) d'origine de l'attaque.
- l'adresse (ou les adresses) visées par l'attaque.
- le nom de la source ayant détecté l'attaque.
- le type de la source : unknow, ads, afs, coda, dfs, dns, hosts, kerberos, nds, nis, nisplus, nt, wfw
- la localisation de la source.

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

- un degré de fiabilité de la source : unknown, yes, no.
- l'interface réseau de la source.
- les nom, port et protocole de la source.

Notez bien que toutes ces informations n'ont pas à être renseignées pour qu'une règle soit valide !

Exemple :
```
regex=no such user; class.name=Invalid User; impact.completion = failed;
impact.type = other; impact.severity = medium; impact.description = Someone
tryed to log in using a non existing user;
```

La séquence "no such user" sera recherchée dans les fichiers définis comme étant à surveiller, sa découverte déclenchant une alerte pour laquelle certains paramètres ont été ensuite précisés.

Autre exemple (logs ipfw) :
```
regex=ipfw: (\d+) Deny (TCP|UDP) ([\d\.]+):(\d+) ([\d\.]+):([\d]+) in via (\w+);
class.name=Packet dropped by firewall; impact.completion=failed;
impact.type=other; impact.severity=medium; impact.description=Denied incoming
packet (rule #$1) $2 $3:$4 -> $5:$6 on interface $7;
source.node.address.address=$3; source.service.port=$4;
source.service.protocol=$2; target.node.address.address=$5;
target.service.port=$6; target.service.protocol=$2; source.interface=$7;
```

On voit bien ici que la ligne de journalisation ipfw est découpée de façon à construire un message que la sonde enverra au(x) contrôleur(s).

4.4. Configuration de l'interface web.

La configuration de l'interface web - hors celle de PHP et d'Apache que nous considèrerons comme effectuée - se fait simplement en renseignant les paramètres de connexion aux deux bases prelude et prelude-frontend, ainsi que les chemins d'accès aux librairies AdoDB et PHPlot (fichier `db/variables.inc.php`).

Une fois les composants configurés, nous pouvons préparer leur lancement.

5. Exploitation

Les composants Prelude sont maintenant installés là où il le faut et configurés comme il le faut, il est donc temps de les lancer.

Première étape : la création des clefs sur les contrôleurs compilés avec le support SSL.

5.1. Création des clefs des contrôleurs

Avant de créer la clef du contrôleur, celui-ci devra bien entendu avoir été installé.

Pour créer cette clef, il faut lancer la commande `/usr/local/bin/manager-adduser`. Lors de la première exécution, l'absence de clef contrôleur sera détectée et celle-ci sera créée (stockée dans `/usr/local/etc/prelude-manager`).

Retenez bien que chaque contrôleur, même s'il n'est destiné qu'à servir de relais, doit avoir sa clef propre. La commande manager-adduser doit donc être exécutée après chaque installation d'un nouveau contrôleur.

Notez enfin que ces clefs, tout comme les certificats des sondes, permettront non seulement l'authentification des composants, mais aussi le chiffrement des échanges de messages, ce qui

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

peut se révéler très utile si vous désirez que ces échanges puissent se faire sur des portions de réseaux non sûres ou à travers Internet entre deux sites distants.

5.2. Lancement du contrôleur

Une fois sa clef générée, le contrôleur est lancé grâce à la commande suivante : `/usr/local/bin/prelude-manager -d` (dans le cas d'un contrôleur pourvu d'un fichier de configuration dûment renseigné, il est possible sinon de passer en argument la quasi-totalité des paramètres que peut contenir le fichier de configuration).
Le contrôleur s'exécute maintenant en arrière plan en mode démon.

Notez bien que dans le cas d'une journalisation dans une base de données, le SGBD doit également avoir été lancé.

5.3. Enregistrement des composants

Les composants - et tout particulièrement les sondes - ne peuvent communiquer entre eux que s'ils ont préalablement été enregistrés. Cette phase d'enregistrement garantit que seul un composant légitime dialoguera avec les contrôleurs.

Pour enregistrer un composant, il faut procéder de la manière suivante :

- Une fois installé, tenter de le lancer :
  `/usr/local/bin/prelude-nids -i eth0 -d pour une sonde réseau.`
Si la sonde n'a pas été enregistrée auprès du contrôleur défini dans son fichier de configuration, un message d'avertissement terminera le processus de lancement : ce message contient la commande exacte et ses arguments qu'il vous faudra lancer.
  `sensor-adduser --sensorname prelude-nids --uid 0 --manager-addr x.x.x.x`

La commande sensor-adduser prend en charge l'enregistrement côté client de la sonde réseau. L'argument --sensorname définit le type de composant qui va être déclaré (valeurs : prelude-nids, prelude-lml, prelude-manager). L'argument --uid est tout simplement l'UID de l'utilisateur ayant lancé la commande (ici root) et enfin --manager-addr l'adresse du contrôleur auprès duquel va être enregistrée la sonde.

- dans le même temps, sur le contrôleur, il faut exécuter la commande manager-adduser : cette commande génèrera un mot de passe à usage unique (one-shot password) et se mettra alors en attente de réception des données en provenance du composant. Notez le mot de passe, il vous sera demander sur le composant durant la phase d'enregistrement.

- de nouveau sur le composant, taper Entrée pour signifier à la commande sensor-adduser que le contrôleur est prêt pour l'enregistrement. Laissez-vous ensuite guider par les retours de la commande, entrez le mot de passe fourni par le contrôleur. En fin et en cas de réussite de l'enregistrement, la commande manager-adduser se termine sur le contrôleur, et la commande sensor-adduser sur le composant.

5.4. Lancement d'une sonde réseau

Une fois enregistrée, la sonde réseau se lance de la façon suivante :
`/usr/local/bin/prelude-nids -i eth0 -d`

Le paramètre -i doit être utilisé pour préciser l'interface sur laquelle doit être analysé le trafic.
Le paramètre -d demande à la sonde de s'exécuter en arrière-plan en mode démon.

5.5. Lancement de la sonde locale

Une fois enregistrée, la sonde réseau se lance de la façon suivante :
`/usr/local/bin/prelude-lml -d`

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..

La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne
le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

Une fois encore, le paramètre -d demande à la sonde de s'exécuter en arrière-plan en mode démon.

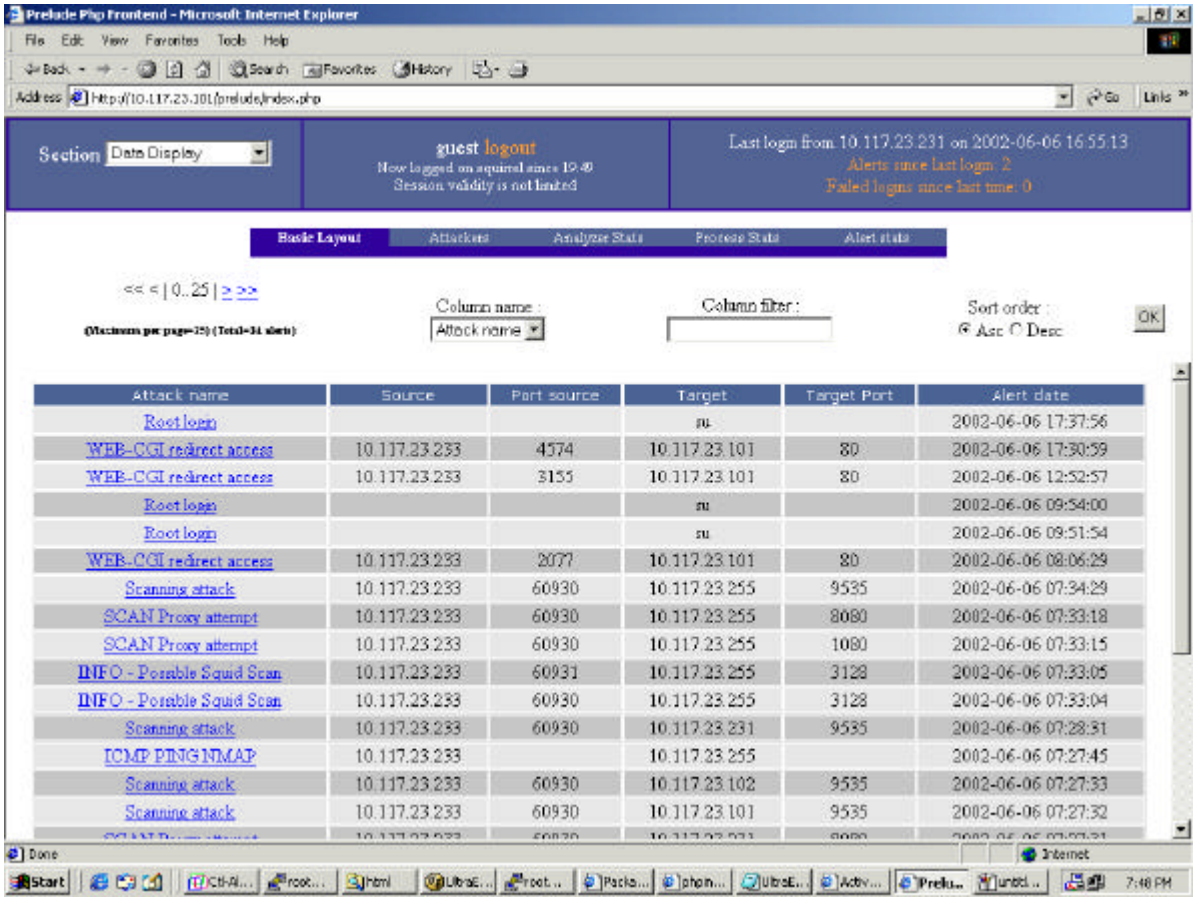
5.6.Interface Web

L'interface web de Prelude ne se lance pas à proprement parler : étant destinée à être installée sur un serveur Web avec PHP, il suffit de configurer ledit serveur pour rendre l'interface Prelude accessible (soit une URL, soit un hôte virtuel).

Notez que l'interface n'a pas à être installée sur le serveur hébergeant le contrôleur et la base SQL, mais que vous prenez le risque de faire transiter en clair les alertes contenues dans la base Prelude : utilisez alors un serveur supportant le protocole HTTPS si vous optez pour ce schéma (contrôleur + base sur un serveur, interface web sur un autre).

Notez enfin que l'accès à l'interface est contrôlé et qu'il faudra à l'exploitant un identifiant et le mot de passe associé pour pouvoir consulter les données issues des alertes Prelude.

La page d'accueil (après authentification) de l'interface web de Prelude ressemble actuellement à ceci :



© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.

6. Conclusion

Avec Prelude, on peut dire qu'un pas de géant a été franchi en matière d'offre sous licence GPL d'outils de sécurité. (Sans trop s'engager, on peut même retirer « sous licence GPL »...)

Prelude-IDS s'insère facilement et naturellement dans des réseaux de taille moyenne (ou plus) et/ou hétérogènes et son architecture permet toutes les audaces (déploiement en cascades, managers multiples, SGDBs dédiés, etc…).

On peut cependant regretter qu'il manque encore à cet IDS prometteur un mécanisme de gestion des configurations des sondes, qui permettrait à l'administrateur de diffuser et mettre à jour aisément la configuration de chacun des composants de l'IDS, mais ce « défaut » est commun à la majeure partie si ce n'est l'intégralité des IDS issu du monde du logiciel dit Libre.

La prochaine étape sera le développement d'utilitaires de contre-mesures permettant par exemple l'adaptation de règles de filtrage (firewalls ou routeurs) en fonction des alertes remontées par les sondes.

Il serait également souhaitable de réfléchir à l'interfaçage des contrôleurs avec des logiciels tiers commerciaux, ce qui permettrait d'unifier le système de journalisation et de visualisation des alertes de sécurité.

Enfin, il reste encore des choses à faire du côté de la corrélation des alertes : une console dédiée à l'analyse des tendances à moyen/long terme des types d'alertes par exemple reste à développer.

Quoiqu'il en soit, Prelude est un produit à suivre… et à tester au plus vite ☺ !

Liens utiles

Logiciels cités dans ce document

Prelude-IDS	http://www.prelude-ids.org
Signatures Snort	http://www.snort.org/dl/rules/
Snort	http://www.snort.org
FireStorm	http://www.scaramanga.co.uk/firestorm/index.html
Ntsyslog	http://ntsyslog.sourceforge.net
PCRE	http://www.pcre.org
PHP	http://www.php.net
Apache	http://www.apache.org
AdoDB	http://php.weblogs.com/adodb

Autres liens intéressants

WhiteHats / ArachNIDS	http://www.whitehats.com
CVE	http://cve.mitre.org

21/06/2002

© 2002 – Guillaume Arcas – Tous droits réservés y compris pour l'U.R.S.S..
La reproduction totale ou partielle du présent document est autorisée à condition que la copie mentionne le nom et l'adresse électronique de l'auteur original et qu'aucune modification n'ait été apportée au document original.