Présentation de la plateforme IDS Prelude

Système de Détection d'Intrusion Hybride

> IDS

> Définition

« Un**Système de Détection d'Intrusion** (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une action de prévention sur les risques d'intrusion. »*Wikipedia*

> Il existe deux grandes familles d'IDS...

- Les **NIDS** (Network Based Intrusion Detection System)

Ils surveillent l'état de la sécurité au niveau du **réseau** (ex : Snort, Shadow, etc.).

- Les **HIDS** (Host Based Intrusion Detection System)

Ils surveillent l'état de la sécurité au niveau des **machines** (ex : Samhain, Portsentry, etc.)

> NIDS (Network based IDS)

Les NIDS analysent le trafic réseau. En général, ils sont composés :

• d'une sonde qui "écoute" sur le segment de réseau à surveiller ; et

• d'un moteur qui réalise l'analyse du trafic afin de détecter des signatures d'attaques ou les divergences face à une politique de référence.

> Avantage des NIDS

• Couverture de l'ensemble du réseau
• Support pour la détection d'un nombre d'attaque conséquent

> Inconvénients des NIDS

• Taux de faux positifs élevé
• Analyse des données cryptées impossible
• Traitement superficiel de l'information (contrainte de performance)
• La grande variété de systèmes d'exploitation complique le mimétisme de la part des NIDS

> HIDS (Host based IDS)

Les HIDS analysent le fonctionnement ou l'état des machines sur lesquelles ils sont installés dans le but de détecter des attaques ou certains états.

Ils ont pour mission :
- d'analyser des journaux systèmes,
- de contrôler l'accès aux appels systèmes,
- de vérifier l'intégrité des systèmes de fichiers, etc.

> Avantages des HIDS

- Pas ou peu de faux positifs.
- Pas ou peu d'adaptation à la politique de sécurité en utilisation.

> Inconvénients des HIDS

- Complexité du déploiement

> NIDS ou HIDS : Imparfait, mais complémentaire !

Pour améliorer la sécurité des infrastructures, il est apparu nécessaire de regrouper le traitement des informations en provenance des NIDS (réseau) et des HIDS (machines) afin de tirer partie des deux types de détection d'intrusion à la fois.

> Naissance de l'IDS Hybride (à la fois NIDS & HIDS)

- Il bénéficie à la fois des avantages des NIDS et des HIDS
- Il permet d'accèder à une vision globale de l'état des systèmes.

Les sondes HIDS et/ou NIDS sont placées en des points stratégiques de l'infrastructure.

Toutes ces sondes remontent alors des alertes dans un format standardisé vers un concentrateur qui va centraliser et stocker les données.

> Avantages des IDS Hybrides

• Bénéficiant du support des HIDS, ils sont insensibles aux problèmes rencontrés par les NIDS.

• Multipliant les rapports d'événements, leurs capacités de corrélation, d'établissement de scénario d'attaques sont bien plus importantes que les systèmes n'analysant qu'un seul type d'information.

• D'autre part, s'il est facile pour un individu malveillant de contourner la détection des attaques par une sonde unique, il devient exponentiellement plus difficile de contourner les protections quand de multiples mécanismes de protection s'additionnent.

> Conditions aux IDS Hybrides :

➨ Adoption d'un language de communication commun à toutes les sondes

C'est ici que l'utilisation d'un standard d'échange de messages de détection d'intrusion, **le standard IDMEF**, prend toute son importance.

> IDMEF (Format d'Echange de Messages de Détection d'Intrusion)

IDMEF définit le format de données pour l'émission d'alertes par les Systèmes de Détection d'Intrusion. Le standard IDMEF a été créé dans le but de permettre l'interopérabilité entre les différents IDS.

Statut actuel d'IDMEF :

Après une longue attente de synchronisation avec l'IANA (Internet Assigned Numbers Authority) pour l'allocation d'un RFC et d'un numéro de port IDXP (référencé depuis le draft IDMEF), IDMEF est finalement officialisé "expérimental" (publié, stabilisé pour implémentation) par le RFC 4765.

Language) qui pose un certain nombre de problèmes liés à la rapidité de traitement des alertes.

➨ **Pour cette raison:** l'IDS Prelude dont nous allons bientôt parler, implémente une version d'IDMEF reposant sur le langage C. La compatibilité est assurée à l'aide d'un module Prelude, capable de convertir une alerte IDMEF-Prelude au format IDMEF-XML.

> Prelude Hybrid IDS

Prelude est hybride, c'est une plateforme IDS Open Source disponible sous licence GPL.

> Plateforme IDS

Prelude est un Système de Détection d'Intrusion autonome qui administre aussi, de façon centralisée, l'ensemble du dispositif de sécurité quel que soit le nombre de composants, leur marque ou leur licence.

> Fonctionnalités Prelude

- Détection d'Intrusion réseau (NIDS)
- Détection d'Intrusion machines (HIDS)
- Correlation d'événements
- Scanner de vulnérabilités
- Récupération des alertes depuis routeurs, pares-feu & AntiVirus
- Vérification d'intégrité des fichiers
- Analyse comportementale d'individus malveillants (honeypot),
- Etc.

> Système distribué

Le système Prelude est distribué, c'est à dire, composé de multiples éléments modulables répartis sur l'ensemble de l'infrastructure.

> Composants du système

- **Le concentrateur** *ou manager Prelude* est un serveur haute disponibilité recevant les messages provenant des différentes sondes. Il est capable de stocker, relayer, ou filtrer ces messages
- **L'agent de correlation Prelude**, lit les alertes reçues par un concentrateur, et émet des alertes de correlations lorsqu'un ensemble d'évenements peut s'associer.
- **La bibliothèque Prelude**, *ou libprelude,* automatise la communication sécurisée (SSL) entre les sondes et les concentrateurs. Elle fournit les fonctionalités nécessaires à l'émission d'événements IDMEF dans Prelude
- **La bibliothèque PreludeDB**, ou libpreludedb, assure l'abstraction pour l'accès aux bases de données contenant des messages IDMEF Prelude
- **Prewikka**, l'interface de visualisation des évenements sécurité Prelude

- **Et, les sondes...**

> *Exemple de sondes supportées par Prelude*

• **Snort** est un NIDS dont l'analyse est basée sur des signatures ;

• **Prelude-LML** est une sonde d'analyse de journaux système, c'est un HIDS. Il est capable de s'interfacer à tout type d'application émettant des alertes de sécurité dans un "journal système" : netfilter, arsecuri
pix, routeur cisco, vpn cisco, clamav, OpenSS
nagios, ipfw, Linux-Pam, postfi

• **Prelude-RE**

Le nombre de sondes est potentiellement illimité : tout système de sécurité a la possibilité d'exporter les éléments qu'il détecte dans le système Prelude.

egrité des fichiers système ;

est une sonde d'analyse de l'état des machines ;

• **Nepenthes** est une solution pour détecter et collecter les vers et autres malwares (virus, spyware, cheval de trois, etc) se propageant sur différents systèmes

• **Sancp** est un outil conçu pour collecter des informations statistiques concernant l'activité réseau. Il peut être utilisé pour qualifier et notifier un trafic réseau suspect.

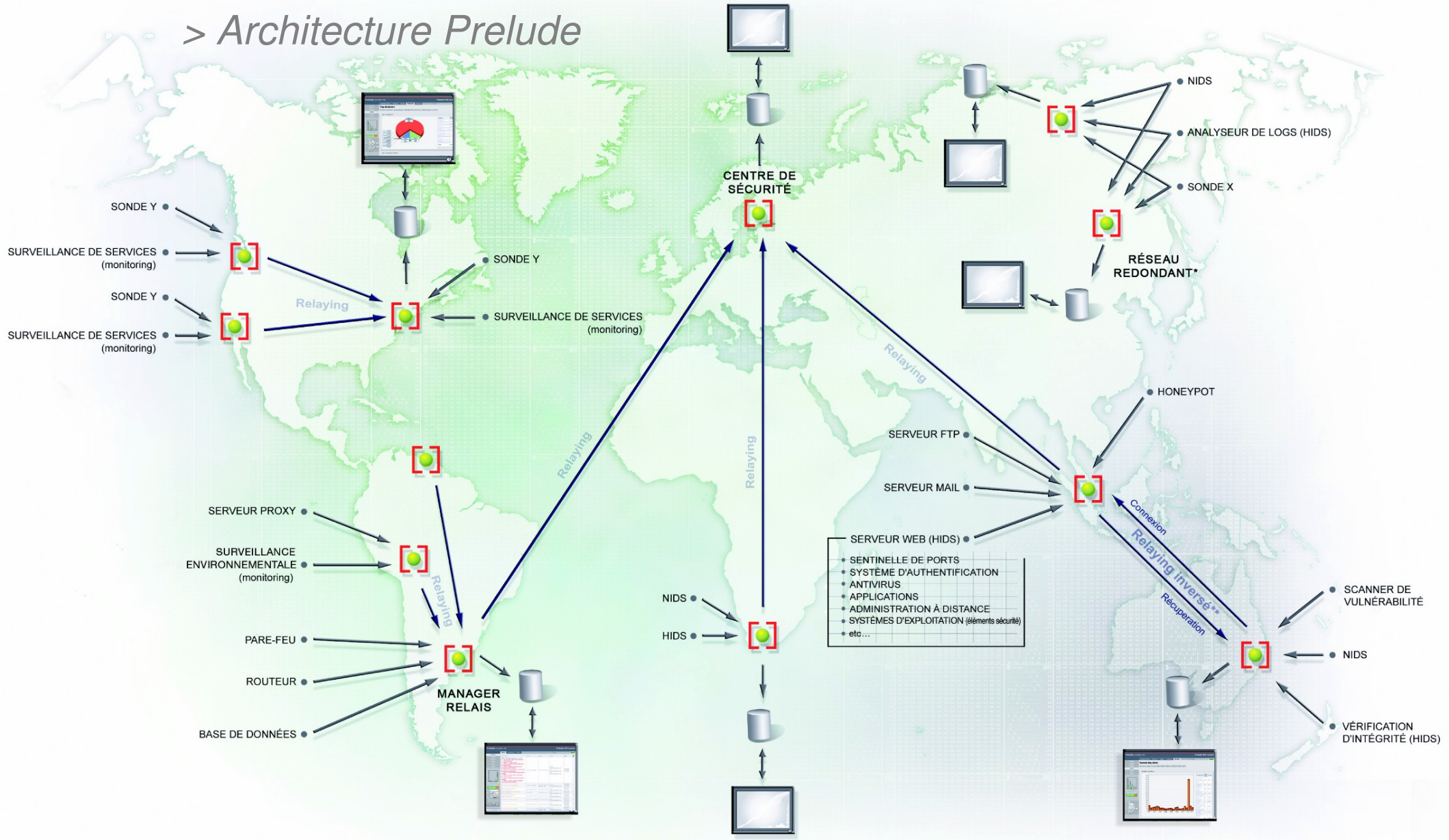

```
# PAX: From 1.2.3.4: execution attempt in: /usr/lib/paxtest/shlibtest.so, 25891000-25892000 00001000
# PAX: terminating task: /usr/bin/localedef(localedef):5208, uid/euid: 0/0, EIP: BFF4C330, ESP: BFF4C21C

regex=From (\S+): execution attempt in:; \
 add_context=PAX_OVERFLOW_SOURCE; \
 source(0).node.address(>>).address = $1; \
 silent; last;

regex=terminating task: ([^(]+)\(([^)]+)\):(\d+), uid/euid: (\d+)/(\d+); \
 optional_context=PAX_OVERFLOW_SOURCE; \
 destroy_context=PAX_OVERFLOW_SOURCE; \
 classification.text=Possible buffer overflow; \
 id=402; \
 revision=2; \
 analyzer(0).name=PAX; \
 analyzer(0).manufacturer=www.grsecurity.net; \
 analyzer(0).class=Memory Violation; \
 assessment.impact.completion=failed; \
 assessment.impact.type=file; \
 assessment.impact.severity=high; \
 source(0).process.path = $1; \
 source(0).process.name=$2; \
 source(0).process.pid=$3; \
 source(0).user.category=application; \
 source(0).user.user_id(0).type=current-user; \
 source(0).user.user_id(0).number=$4; \
 source(0).user.user_id(1).type=original-user; \
 source(0).user.user_id(1).number=$5; \
 assessment.impact.description=A possible buffer overflow occured in $1. You should consider this an
```

> IDS > IDS Hybride > Prelude IDS > Architecture

> Architecture Prelude



SONDE X: rendue compatible Prelude à la demande du client
SONDE Y: développée par le client

MANAGER PRELUDE (concentrateur)

IHM PREWIKKA

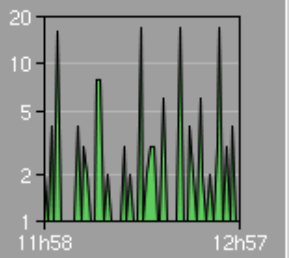
BASE DE DONNEES

connexions sécurisée (SSL) entre tous les modules

PreludeIDS Technologies — **Prelude console**

Alerts | Heartbeats | Filters — *admin* on Thursday October 06 2005 — logout

- Events
- Agents
- Tickets
- Stats
- Users
- About



Sensors availability:

4	1

Filter: | Step: 1 Hours | Tz: Frontend localt | Limit: 50 apply

2005-10-06 11:57:55
2005-10-06 12:57:55
+02:00

prev | current | next

<< | < | > | >>

1 ... 30 (total:30)

Classification	Source	Target	Sensor	Time
1 x **Multiple User Login** (**succeeded**) 1 x **User Logout** (**succeeded**) 1 x Mail server suspicious access (failed) 1 x User login successful (**succeeded**)	arwen.prelude-ids.org [redacted]	awale.prelude-ids.org [redacted] user: yoann (1000)	Postfix (awale.prelude-ids.org) samhain (awale.prelude-ids.org) sshd (awale.prelude-ids.org)	12:57:04 - 12:48:30 #6 opened by admin new ticket
81 x UDP packet dropped (failed)	[redacted]:138/udp	[redacted]:138/udp interface: eth0	netfilter (awale.prelude-ids.org)	12:55:54 - 12:02:36 new ticket
IMAP PCT Client_Hello overflow attempt (vendor-specific:url, cve:2003-0719, bugtraqid:10116)	[redacted]:63105/tcp	[redacted]:993/tcp	snort (awale.prelude-ids.org)	12:55:34 new ticket
2 x **WEB-MISC PCT Client_Hello overflow attempt** 2 x TCP packet dropped (failed) 1 x WEB-MISC robots.txt access	[redacted]:65159/tcp	[redacted]:443/tcp interface: eth0	netfilter (awale.prelude-ids.org) snort (awale.prelude-ids.org)	12:55:14 - 12:29:50 #5 opened by admin new ticket
5 x User authentication successful (**succeeded**)	user: 1000	awale.prelude-ids.org [redacted] user: root	PAM (awale.prelude-ids.org)	12:55:12 - 12:50:03 new ticket
WEB-MISC robots.txt access (vendor-specific:url)	[redacted]:55619/tcp	[redacted]:80/tcp	snort (awale.prelude-ids.org)	12:53:57 new ticket
3 x WEB-MISC robots.txt access	[redacted]:31379/tcp	[redacted]:80/tcp	snort (awale.prelude-ids.org)	12:53:45 - 12:33:30 new ticket
9 x UDP packet dropped (failed)	[redacted]:138/udp	[redacted]:138/udp interface: eth0	netfilter (awale.prelude-ids.org)	12:48:20 - 12:00:19 new ticket
10 x UDP packet dropped (failed)	[redacted]:137/udp	[redacted]:137/udp interface: eth0	netfilter (awale.prelude-ids.org)	12:46:39 - 11:58:26 new ticket
WEB-MISC robots.txt access (vendor-specific:url)	[redacted]:42753/tcp	[redacted]:80/tcp	snort (awale.prelude-ids.org)	12:45:41 new ticket
5 x UDP packet dropped (failed)	[redacted]:53/udp	[redacted]:33903/udp interface: eth0	netfilter (awale.prelude-ids.org)	12:45:29 - 12:00:15 new ticket
4 x TCP packet dropped (failed)	[redacted]:53533/tcp	[redacted]:25/tcp	netfilter	12:45:20 - 12:44:59

> Conclusions

- En uniformisant les données émises par les différentes sondes ;
- En permettant de les stocker ensemble ;
- En permettant de les trier et de les corréler ;

...Prelude, au travers du standard IDMEF, permet la multiplication des formes de détection employées sur une infrastructure.

La multiplication des sondes et la disponibilité d'un outil centralisé d'analyse rend beaucoup plus difficile pour un individu malveillant de passer outres les différents systèmes de protection.

L'ajout de sondes Prelude au coeur de la distribution AMON permettrait d'automatiser et de faciliter l'installation de Prelude. Les utilisateurs AMON bénéficieront ainsi de fonctionnalités de surveillance de l'infrastructure et de ses systèmes.

> Liens

- **Projet Prelude :** http://www.prelude-ids.org
- **PreludeIDS Technologies SARL :** http://www.prelude-ids.com

Contact : info@prelude-ids.com

- **Standard IDMEF :** http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt
- **Snort :** http://www.snort.org
- **Samhain :** http://la-samhna.de/samhain/
- **Nessus :** http://www.nessus.org
- **Nepenthes :** http://nepenthes.mwcollect.org
- **Sancp :** http://www.metre.net/sancp.html

Merci pour votre attention...

