Ecole d'ingénieurs du Canton de Vaud

Tél. : + 41 24 423 21 11
Fax : + 41 24 425 00 50
info@eivd.ch
http://www.eivd.ch

Travail de diplôme 2004

Département Electricité et Informatique

Ecole d'ingénieurs du Canton de Vaud
Route de Cheseaux 1, case postale
CH - 1401 Yverdon - les - Bains

SIMS Security Management System (orienté Web)

Problématique :

La gestion de la sécurité est devenue indispensable au même titre que la gestion du réseau lui-même. On peut même prétendre que la gestion de la sécurité est désormais le souci majeur du gestionnaire du réseau de l'entreprise. Ce projet va se focaliser sur le développement d'un gestionnaire (Manager) de sécurité appelé SIMS (Security Intrusion Management System) disposant d'agents intelligents ouverts (sondes réseaux et analyseurs de logs, regroupés sous l'appellation IDS "Intrusion Detection System").

SIMS orienté Web est donc spécialisé dans le domaine de l'analyse des tentatives d'intrusions sur des serveurs Web détectées par des plates-formes de type Firewall et IDS.

Pour ce faire, l'application d'analyse (appelée moteur de corrélation) devra être capable de récolter les informations des différentes sondes, de les traiter (regrouper celles communes à une même attaque) et de fournir un résumé des attaques détectées.

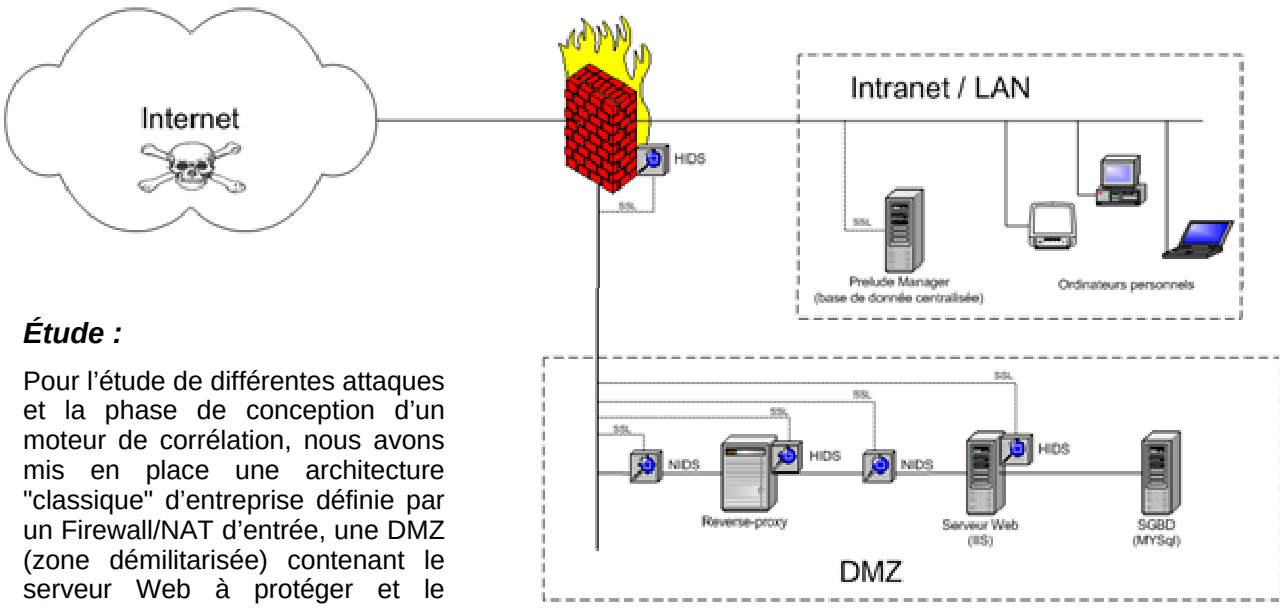
De plus, le serveur Web est protégé par un reverse-proxy Squid couplé avec Dansguardian (deux produits Open Source) permettant de protéger et filtrer les requêtes HTTP émises vers le serveur Web. En effet, le reverse-proxy se fera passer pour le serveur Web auprès des clients et fonctionnera comme cache pour les pages statiques et les images.

Les alarmes émises par les différentes sondes (IDS) sont rapatriées vers la base de donnée d'un manager centralisé Open Source (Prelude Manager) via un flux sécurisé (SSL).

Conception :

Après l'étude de différentes possibilités de recherche de similitudes entre les alarmes levées par les sondes les plus proches du serveur Web (donc les plus critiques) nous avons défini un graphe d'états permettant d'illustrer les différentes étapes de corrélation nécessaires.

Nous avons ensuite implémenté cette méthodologie sous forme de site Web dynamique en Perl, permettant ainsi son intégration dans l'interface existante de Prelude.



Étude :

Pour l'étude de différentes attaques et la phase de conception d'un moteur de corrélation, nous avons mis en place une architecture "classique" d'entreprise définie par un Firewall/NAT d'entrée, une DMZ (zone démilitarisée) contenant le serveur Web à protéger et le réseau de l'entreprise (LAN).

Auteur: **Winteregg Joël**
Répondant externe:
Prof. responsable: **Ventura Stefano**
Sujet proposé par: **EIVD - institut TCOM - et l'EIG (projet CCTI)**

Hes·so
Haute Ecole Spécialisée de Suisse occidentale