heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Intégration de la détection d'intrusion dans le tableau de bord de la Sécurité informatique

Contexte

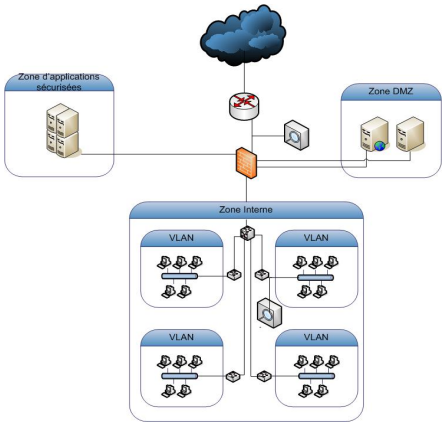
Actuellement la plupart des dirigeants d'entreprises mesurent l'insuffisance des moyens alloués à la sécurité informatique après un dommage plus ou moins critique subi.

Il est donc urgent d'étudier quels indicateurs peuvent êtres créés et présentés à un responsable de sécurité informatique ou à la direction afin de l'aider à prendre des décisions

Ce travail propose dès lors une ébauche de tableau de bord de la sécurité basé sur un indicateur de détection d'étanchéité aux alertes dans une architecture hybride.

Indicateur d'étanchéité aux attaques

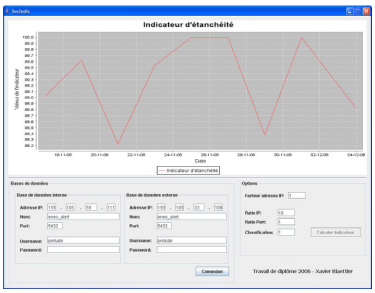
Le but de notre indicateur d'étanchéité aux attaques est de déterminer le niveau de menace interne résiduel en se basant sur la proportion d'attaques externes que l'on retrouve en interne.



Un des objectifs est de mesurer les résultats de la politique de défense actuelle et d'en suivre sa progression sur une durée étendue. L'autre objectif est de servir de benchmark dans le cas de test de nouvelles solutions en tous genres et permettra de quantifier de manière concrète le gain de la nouvelle solution testée.

Représentation de l'indicateur

Le programme fournira un outil de visualisation qui permet d'afficher une tendance de l'indicateur.



De plus, nous aimerions, par le biais de cette application portable, fournir une ébauche d'un futur tableau de bord plus professionnel. Pour cela nous avons essayé de rendre le code le plus réutilisable possible.

Conclusion

Mener à terme ce travail de diplôme fut un véritable challenge. En effet il a fallu acquérir un grand nombre de connaissances nouvelles tout au long du déroulement du projet pour surmonter toutes les difficultés rencontrées. Par contre, cette réalisation permet d'envisager une multitude de domaines d'évolutions possibles (automatisation des mises à jour, contrôle et configuration des sondes automatique).

Technologies utilisées

Linux, Prelude IDS, Snort, PostgreSQL, VMWare, Java

Auteur: **Xavier Blaettler**
Répondant externe: **Christophe Gabioud**
Prof. responsable: **Stefano Ventura**
Sujet proposé par: **Hospices - CHUV**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale