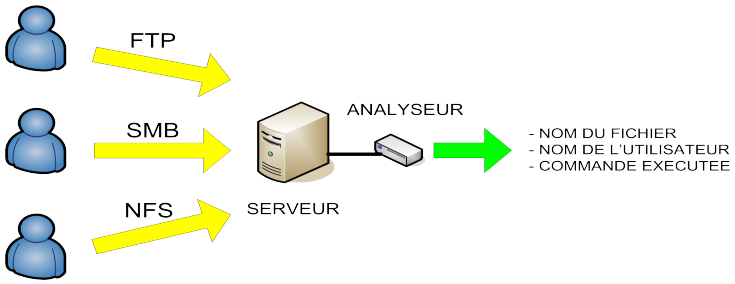
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

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

High Performance Packet Analysis State Machine for Network Security and Compliance Monitoring of Ethernet Traffic



Ce projet a été réalisé en collaboration avec Vigiliti Systems Inc, une start-up de sécurité informatique basée en Californie.

Présentation de Vigiliti Systems Inc.

Vigiliti Systems Inc. est une start-up de la Silicon Valley basée à Santa Clara (CA). Elle développe et vend un produit de sécurité, nommé nLive, pour les réseaux informatiques des entreprises.

Solution apportée par nLive

nLive permet d'avoir une vue de l'activité, passée et présente, sur un réseau informatique. De multiples capteurs analysent l'état du réseaux. Ces capteurs envoient les informations correspondantes au système central de nLive. Ces informations sont ensuite analysées par des algorithmes (intelligence artificielle) afin de détecter toutes anomalies. De ce fait le système ne requière aucune mise à jour d'une base de signature d'attaque ou d'anomalie.

Présentation du projet

Le projet consistait à ajouter une fonctionnalité au produit nLive. Cette fonctionnalité permet d'enregistrer quels fichiers sont accédés et par qui. Et cela qu'il s'agisse d'accès vers le réseau local ou vers l'Internet.

Des algorithmes d'analyse ont été développés pour les protocoles les plus rependus pour l'accès à des fichiers à savoir :

- File Transfert Protocol (FTP)
- Server Message Block (SMB)
- Network File System (NFS)

Le développement de l'algorithme pour chaque protocole, comprenait trois phases :

- Étude du fonctionnement du protocole
- Développement, dans nLive, d'un analyseur du protocole en langage C++
- Contrôles de fonctionnement par simulation

Au final, pour chacun des protocoles, un analyseur indique :

- le nom du fichier accédé
- le nom de l'utilisateur
- la commande exécutée sur le fichier.

Expérience humaine

Ce projet s'est déroulé en Californie dans un climat remarquable de rencontres, d'ouverture et de pragmatisme.

Il n'y a pas de problème, que des solutions. JUST TRY!

Auteur: **Félicien FLEURY | felicien.fleury-at-gmail.com**
Répondant externe: **Saptho NAIR**
Prof. responsable: **Stephan ROBERT**
Sujet proposé par: **Vigiliti Systems Inc.**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale